FIRESCAN

# 방화벽 통합관리시스템
# FIRESCAN 소개

2019년

JMTRUE
(주)제이엠트루

# I. FIRESCAN 소개

# II. FIRESCAN 특장점 및 주요 기능

# III. FIRESCAN 구성 및 사양

JMTRUE
(주)제이엠트루

# I. FIRESCAN 소개

## 1. 도입 배경 및 필요성

1) 분산된 방대한 방화벽 정책의 통합관리 필요

2) 방화벽 정책의 주기적 튜닝 필요

3) 방화벽의 운영 효율성 향상

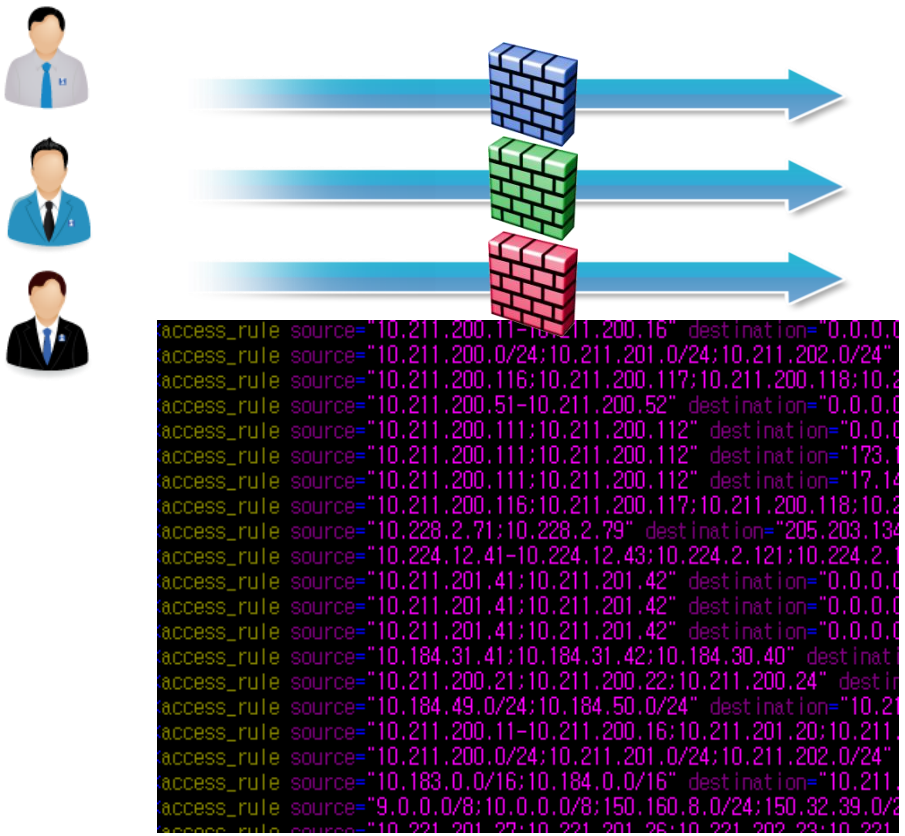
4) 컴플라이언스 대응

## 2. 기대 효과

# 1. 도입 배경 및 필요성

## 분산된 방대한 방화벽 정책 및 로그의 통합분석 체계 필요

"가장 중요한 보안 장비"



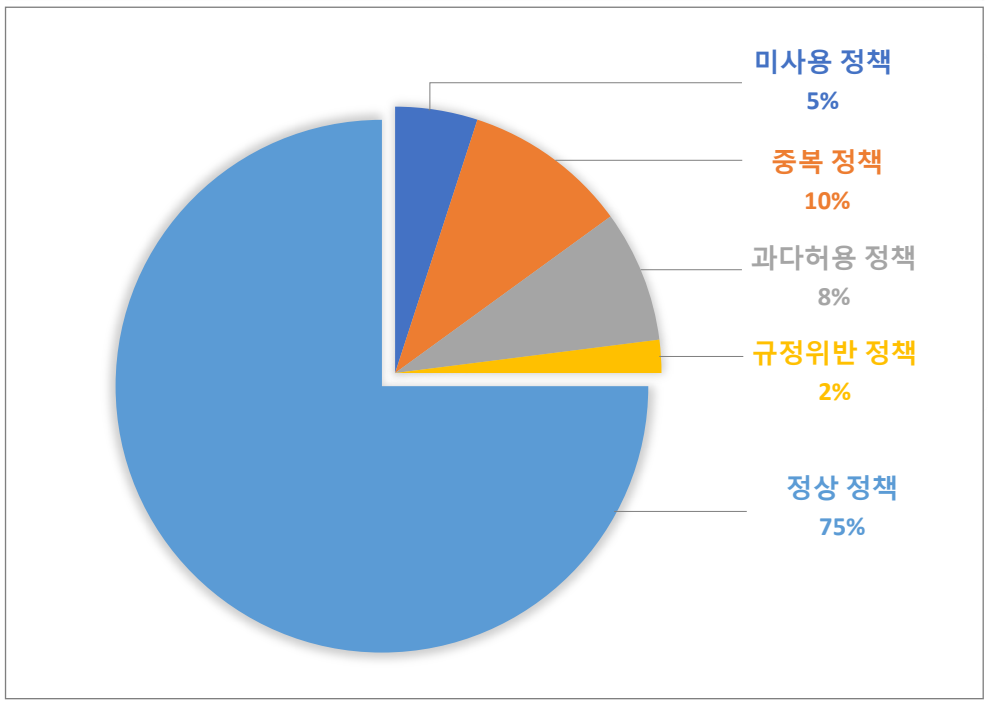

**정책의 복잡성, 대용량 로그, 분산 환경**으로
**『통합 정책 분석 및 최적화 관리』불가능**

방화벽 효율 및 보안성 저하는
주로 **"불필요하거나 잘못 적용된 정책의 방치"** 및
**"주기적 위험 평가 부재"** 로 발생

# 1. 도입 배경 및 필요성

## 방화벽 정책의 주기적 튜닝 필요

### 방화벽 정책 통합 분석 예




(시간이 지남에 따라)
- 정책의 복잡도 증가
- 정책 처리 성능 저하
- 보안 취약점 증가
- 보안 점검, 감사 지적사항

| 분석 내용 | 주요 원인 |
|---|---|
| 미사용 정책 | • 업무 변경/중단, 업무인력 이동 |
| 중복 정책 | • 정책 복잡도 증가, 입력내용 검증 미흡 |
| 과다허용 정책 | • 구축 초기 정밀한 정책 설정 미흡 |
| 규정위반 정책 | • Network Zone 세분화에 따른 대응 미흡, 입력내용 검증 미흡 |



JMTRUE (주)제이엠트루

# 1. 도입 배경 및 필요성

## 방화벽 정책 운영, 관리 업무 효율성 향상 필요

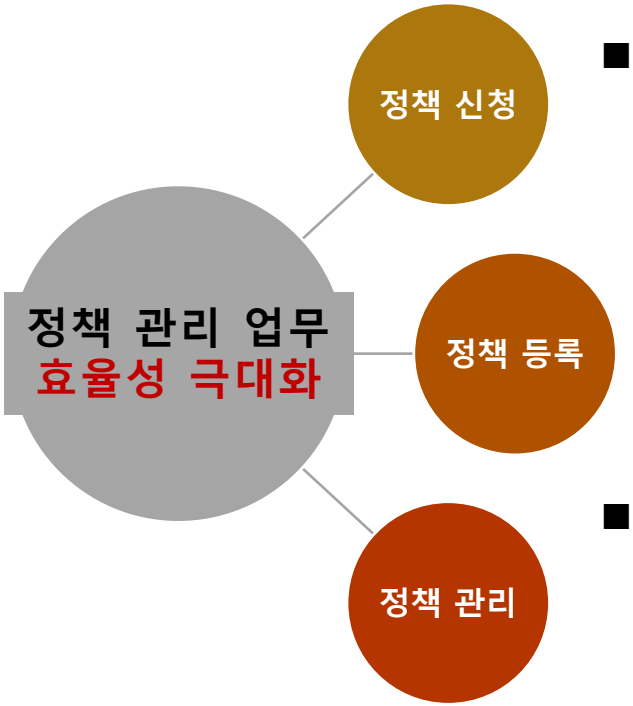
### 방화벽 관리인원은 고정, 운영업무는 점진적 증가


운영 장비 & 등록 정책의 지속적 증가

# 1. 도입 배경 및 필요성

## 방화벽 정책 운영, 관리 업무 효율성 향상 필요

### 업무 효율의 극적 향상을 위한 시스템 구축 필요




■ **정책 신청/승인, 사전검증 프로세스 자동화**

- 정책 신청단계 사전 자동 정책검증
  (규정위반, 중복정책, 경유 방화벽)

■ **시각화 및 정책 등록 무인화**

- 경유 방화벽 및 경로 시각화
- 신청 승인된 정책 등록 작업의 자동화

■ **통합 분석환경 제공 및 사전 알림**

- 정책 및 객체 통합 복합조건 검색
- 위험, 규정위반 정책의 통합 분석
- 미 사용 정책 및 중복정책 등 정책 최적화
- 전체 방화벽 만료 예정정책 사전 인지

# 1. 도입 배경 및 필요성

## 지속적인 컴플라이언스 대응 필요

### 주요 컴플라이언스 이슈 (정보보호 수준진단 혹은 관리체계 인증)

1) **방화벽 정책별 근거 유지 불충분** (신청서와 방화벽 정책 변경이력 매핑)

2) **주기적 위험평가 및 대응활동 미흡**

### 정보보호 관리체계(ISMS) 주요 결함사례 (☞ 정기적 정책(룰) 타당성 검토 및 증적 자료 확보 필요)

1) **ISMS 관련 점검항목**

| 점검 항목 | 점검 내용 |
|---|---|
| **11.2.2 보안시스템 운영** | 보안시스템 유형별로 관리자 지정, 최신 정책 업데이트, 룰 셋 변경, 이벤트 모니터링 등의 운영절차를 수립하고 보안시스템 별 정책 적용 현황을 관리하여야 한다. |

2) **결함 내용**

- **방화벽 정책(Ruleset) 신청 절차 미 준수 (구두, 전화, 메일, 요청 등 담당자 임의변경)**
  - ✓ 정책 신청서와 Ruleset의 생성, 변경, 삭제 이력이 불일치 (사유, 사용기한, 승인여부 등)
- **정기적인 방화벽 정책(Ruleset) 위험성 평가 미수행**
  - ✓ 과도한 내/외부 접속 정책 허용(내부망 in-bounding Any, out-bounding Any), 미승인 정책 사용, 장기간 미사용/중복/사용기간 만료정책 존재 등

# 2. 기대 효과

## 방화벽 정책 통합관리

- ❖ 방화벽 정책 및 로그 통합 분석체계 구축
- ❖ 방화벽 통합 정책 및 객체 복합조건 검색
- ❖ 네트워크 토폴로지 맵 제공 (전체 구성 가시성 확보)
- ❖ 정책 만료예정일 통합 관리

## 최적의 방화벽 정책 상태 유지

- ❖ 중복정책의 주기적 정리
- ❖ 사용률 기반 미 사용 정책 주기적 정리
- ❖ 사용률 기반 주기적 정책순서 재배치


## 방화벽 정책적용 편의성 제공

- ❖ 정책 신청/승인, 사전검증 프로세스 자동화
- ❖ 시각화 및 정책 등록 무인화
  - 정책 별 경유 방화벽 및 네트워크 장비 탐색
  - 정책 적용 전 사전 시뮬레이션
  - 승인/합의 완료된 정책 방화벽 자동 등록
- ❖ 통합 분석환경 제공 및 정책만료일 사전 인지

## 컴플라이언스 대응, 보안강화

- ❖ 내부 관리규정 미 충족 정책 즉시 식별 및 대응
  - 위험 정책 식별 (과다 허용, 중요 서비스 허용 등)
  - 과다허용 정책의 정책 세분화
- ❖ 감독기관 지침 및 법적요건 검증

# II. FIRESCAN 특장점 및 주요 기능

1. 스마트한『정책 최적화』기능
2. 장비 연동 및 네트워크 토폴로지 맵 구성
3. 편리한『사전 시뮬레이션』기능
4. 유용한『정책 현황 분석』기능
5. 유연한『방화벽 정책신청 관리시스템』
6. 시각화된 보고서 지원

# 1. 스마트한『정책 최적화』기능

## 사용률 기반『정책 최적화』및『집중분석』기능 지원

**정책 최적화**

- **중복정책 분석**
  - 동일 정책 — ▪ 동일정책 정리에 활용
  - Shadowed/Redundant 정책 — ▪ 상하위 중복정책 정리에 활용
- **사용률 분석**
  - 미사용 정책 — ▪ 미사용 정책 정리에 활용
  - 정책 순서 재배치 — ▪ 정책 재배치로 처리성능 향상에 활용
- **Application 객체 분석**
  - Application 객체 식별 및 최적화 — ▪ 차세대 방화벽 객체 최적화에 활용
- **집중 분석**
  - 과다허용 정책 실사용 정책 분리 — ▪ 과다허용정책의 정책 세분화에 활용
- **정책 통합**
  - 2개 이상 정책 합산 — ▪ 동일 Zone 정책 통합에 활용

# 1. 스마트한『정책 최적화』기능

불필요한 정책을 줄이기 위한 목적으로 중복 정책을 분석합니다.

**중복정책 분석**

미사용 정책 분석

정책 순서 재배치

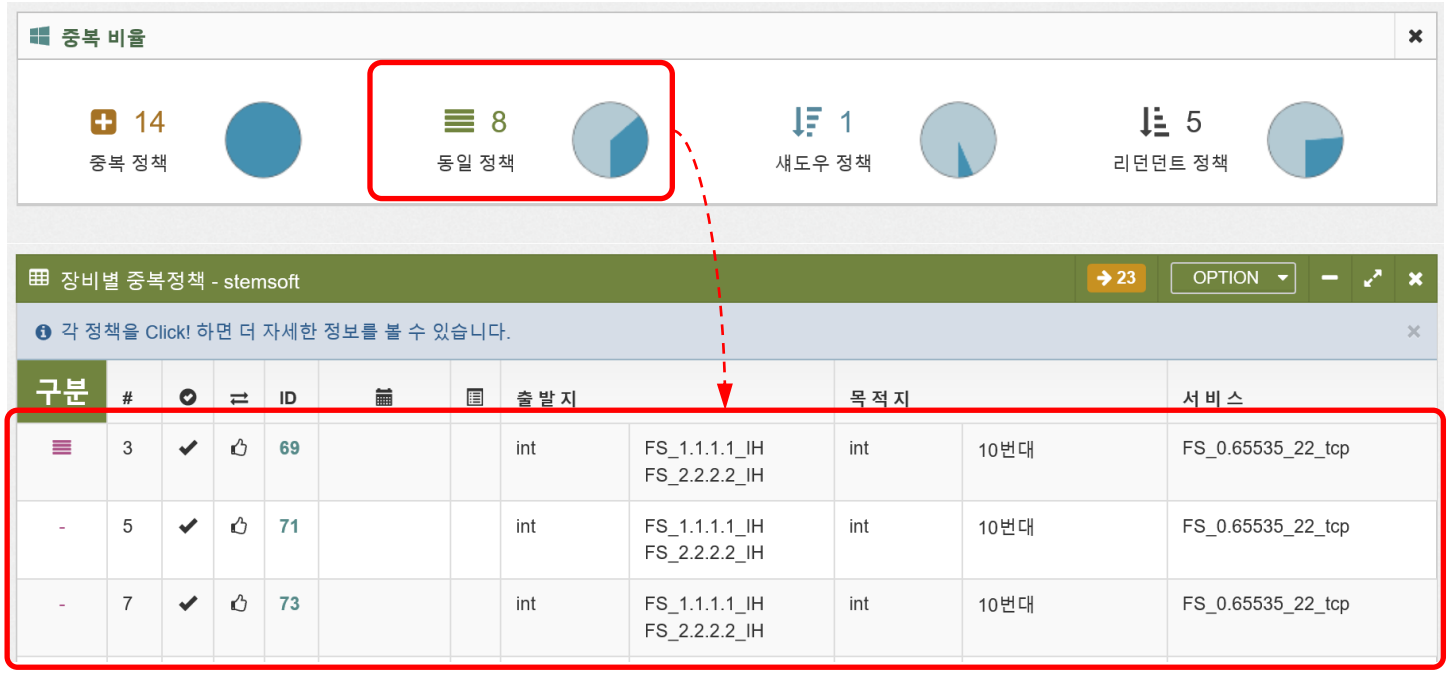
과다허용정책
실사용정책 분리제시

어플리케이션
객체 식별 및 중복 분석

정리대상 정책의
의견 일괄 취합

정책 통합

- **관리자의 착오 / 정책의 복잡성으로 인하여 발생된 중복된 정책 탐지**
  - ✓ 동일 정책
  - ✓ 섀도우 정책
  - ✓ 리던던트 정책



# 1. 스마트한『정책 최적화』기능

방화벽 로그를 기반으로 정책별 사용률 분석을 통해 미사용 정책을 추출합니다.

- 중복정책 분석
- **미사용 정책 분석**
- 정책 순서 재배치
- 과다허용정책 실사용정책 분리제시
- 어플리케이션 객체 식별 및 중복 분석
- 정리대상 정책의 의견 일괄 취합
- 정책 통합

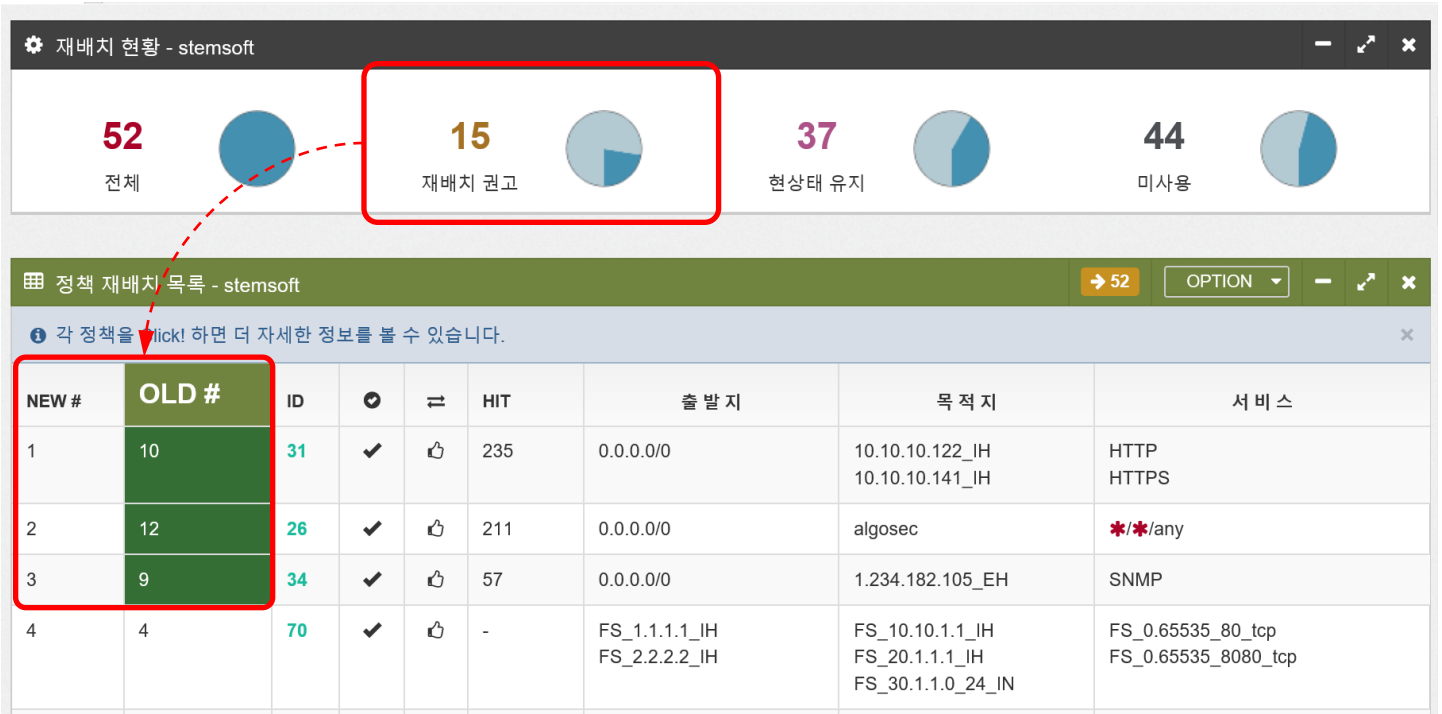
- **방화벽 로그를 분석하여 정책 사용률을 표시**
- **지정한 기간 동안 사용률이 없는 정책 추출**

# 1. 스마트한『정책 최적화』기능

방화벽 처리 효율 향상을 위한 목적으로 정책별 사용률 분석을 통해 사용빈도가 높은 순서로 정책 재배치안을 제시합니다.

- 중복정책 분석
- 미사용 정책 분석
- **정책 순서 재배치**
- 과다허용정책 실사용정책 분리제시
- 어플리케이션 객체 식별 및 중복 분석
- 정리대상 정책의 의견 일괄 취합
- 정책 통합

• **사용빈도 높은 순으로 정책 재배치**

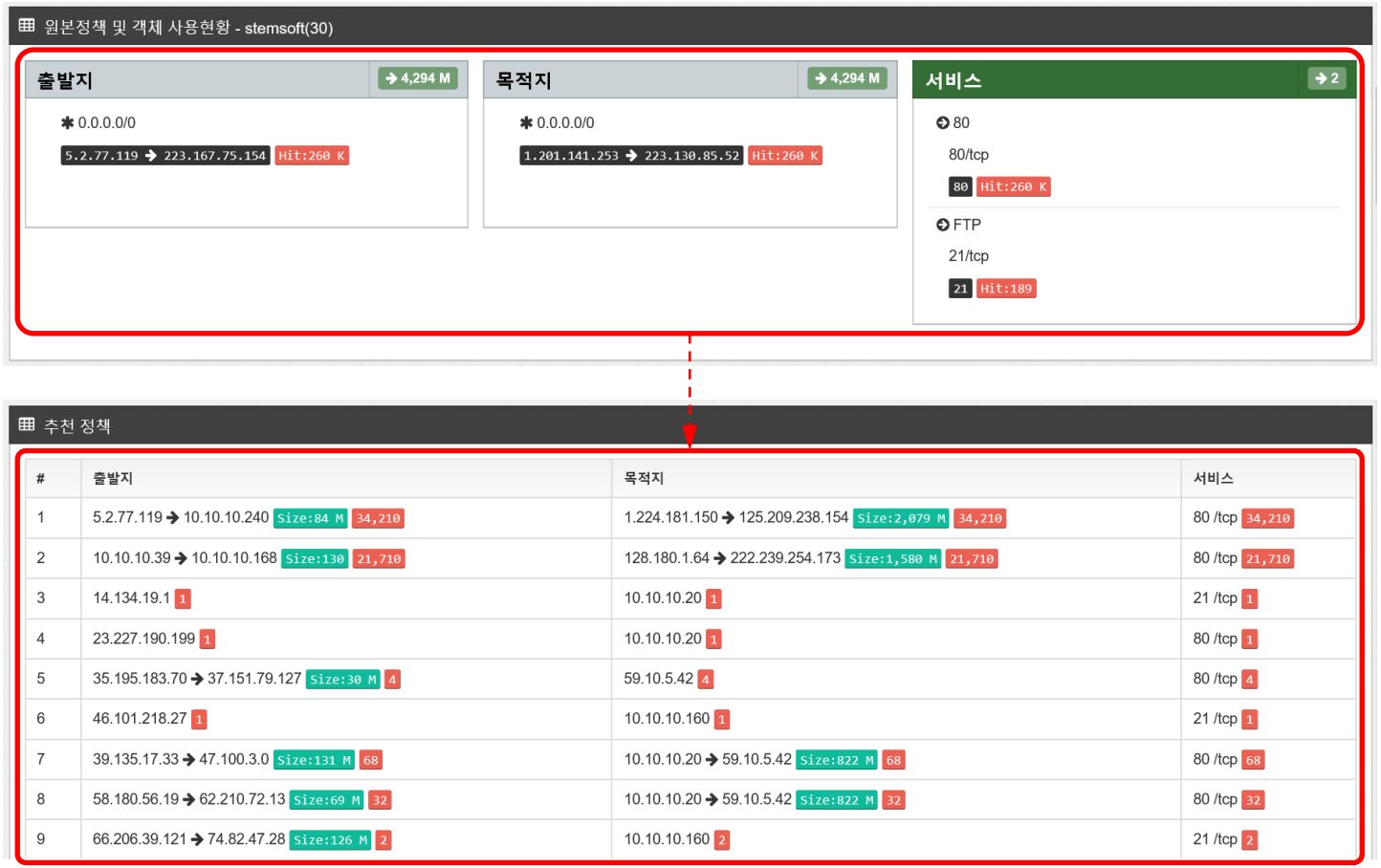


# 1. 스마트한『정책 최적화』기능

사용률 분석을 통해 정책 내 과다허용 대역을 실사용 대역들만으로 분리하여 대체 정책으로 제시합니다.

- 중복정책 분석
- 미사용 정책 분석
- 정책 순서 재배치
- **과다허용정책 실사용정책 분리제시**
- 어플리케이션 객체 식별 및 중복 분석
- 정리대상 정책의 의견 일괄 취합
- 정책 통합

- **정책 내 과다허용 대역을 실사용 대역들만으로 분리하여 대체 정책으로 제시**




| # | 출발지 | 목적지 | 서비스 |
|---|---|---|---|
| 1 | 5.2.77.119 → 10.10.10.240 Size:84 M 34,210 | 1.224.181.150 → 125.209.238.154 Size:2,079 M 34,210 | 80 /tcp 34,210 |
| 2 | 10.10.10.39 → 10.10.10.168 Size:130 21,710 | 128.180.1.64 → 222.239.254.173 Size:1,580 M 21,710 | 80 /tcp 21,710 |
| 3 | 14.134.19.1 1 | 10.10.10.20 1 | 21 /tcp 1 |
| 4 | 23.227.190.199 1 | 10.10.10.20 1 | 80 /tcp 1 |
| 5 | 35.195.183.70 → 37.151.79.127 Size:30 M 4 | 59.10.5.42 4 | 80 /tcp 4 |
| 6 | 46.101.218.27 1 | 10.10.10.160 1 | 21 /tcp 1 |
| 7 | 39.135.17.33 → 47.100.3.0 Size:131 M 68 | 10.10.10.20 → 59.10.5.42 Size:822 M 68 | 80 /tcp 68 |
| 8 | 58.180.56.19 → 62.210.72.13 Size:69 M 32 | 10.10.10.20 → 59.10.5.42 Size:822 M 32 | 80 /tcp 32 |
| 9 | 66.206.39.121 → 74.82.47.28 Size:126 M 2 | 10.10.10.160 2 | 21 /tcp 2 |

# 1. 스마트한『정책 최적화』기능

차세대 방화벽의 어플리케이션 객체 식별 및 중복 분석을 지원합니다.

- 중복정책 분석
- 미사용 정책 분석
- 정책 순서 재배치
- 과다허용정책 실사용정책 분리제시
- **어플리케이션 객체 식별, 중복/사용률 분석**
- 정리대상 정책의 의견 일괄 취합
- 정책 통합

- **차세대 방화벽 어플리케이션 객체 식별 및 중복, 사용률 분석**

장비별 정책 - PA-500

**어플리케이션 객체 식별**

| # | ID | 출발지 | | 목적지 | | 서비스 | 어플리케이션 | UTM사용 |
|---|---|---|---|---|---|---|---|---|
| 1 | stem_test1 | stem<br>wskim | trust | 10.10.10.0/24 | untrust | 0.0.0.0/0 | svc_custom | abb-network-manager<br>adobe-online-office<br>freenet<br>generic-p2p<br>google-duo<br>kakaotalk<br>kakaotalk-base | url-filtering |
| 2 | stem_test1-2 | 2018/12/30 | wskim | trust | FS_6.6.6.7 | any | FS_8.8.8.7 | TCP_4444 | adobe-update<br>any | url-filtering |

**클릭 시 URL 객체 분석결과 제공**

URL 필터

| block-list | action | allow-list | continue category | override category | block category | alert category |
|---|---|---|---|---|---|---|
| naver.com<br>daum.net<br>*.daum.net Hit:6 | block | www.firescan.co.kr Hit:316<br>stemsoft.co.kr | business-and-economy Hit:281 | computer-and-internet-info | adult<br>alcohol-and-tobacco Hit:191 | content-delivery-networks Hit:222 |

naver.com/aaa
daum.net/abc
www.daum.net
*.google.co.kr

**URL 중복 표시**

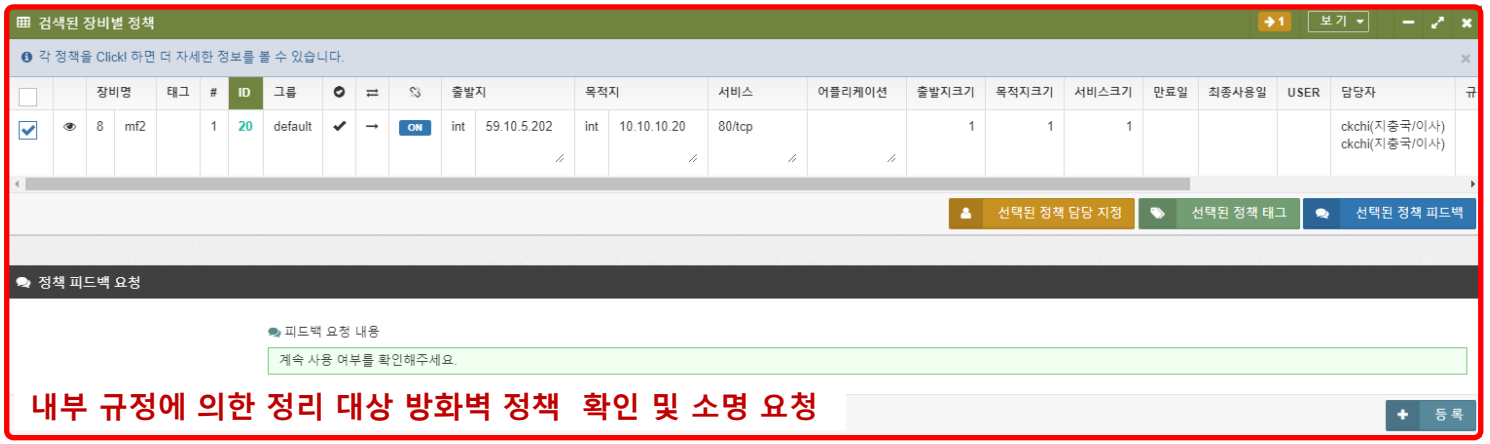
**사용률 표시**

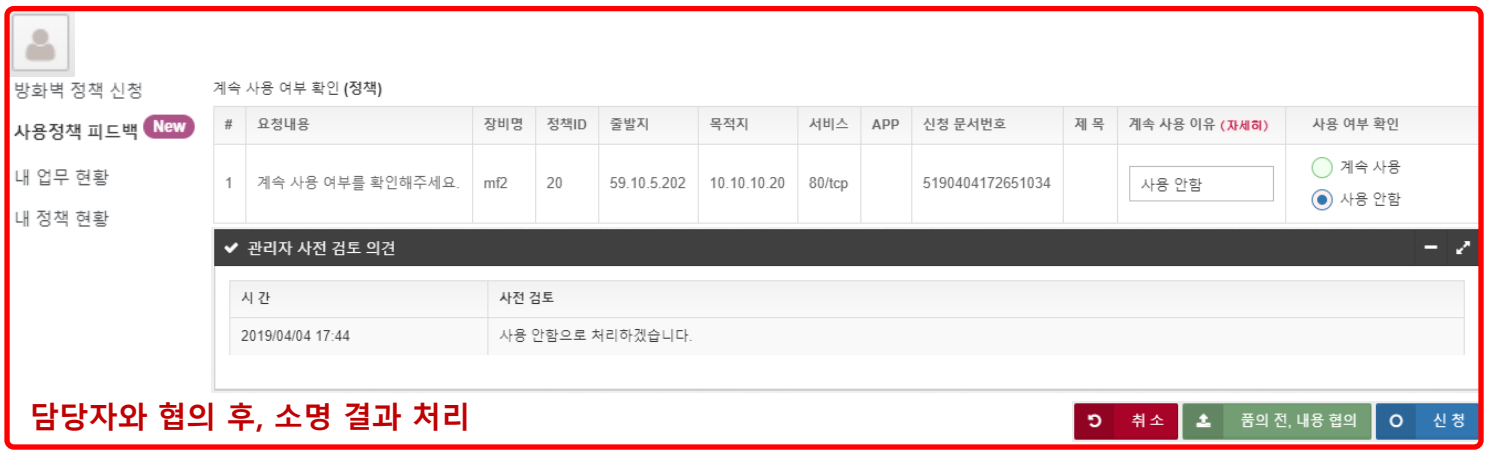
# 1. 스마트한『정책 최적화』기능

정책 최적화에 따른 정리대상 정책의 담당자 소명 및 일괄 취합기능을 제공합니다.

- 중복정책 분석
- 미사용 정책 분석
- 정책 순서 재배치
- 과다허용정책 실사용정책 분리제시
- 어플리케이션 객체 식별 및 중복 분석
- **정리대상 정책의 의견 일괄 취합**
- 정책 통합

- **정책 최적화에 따른 정리대상 정책의 의견 일괄 취합**



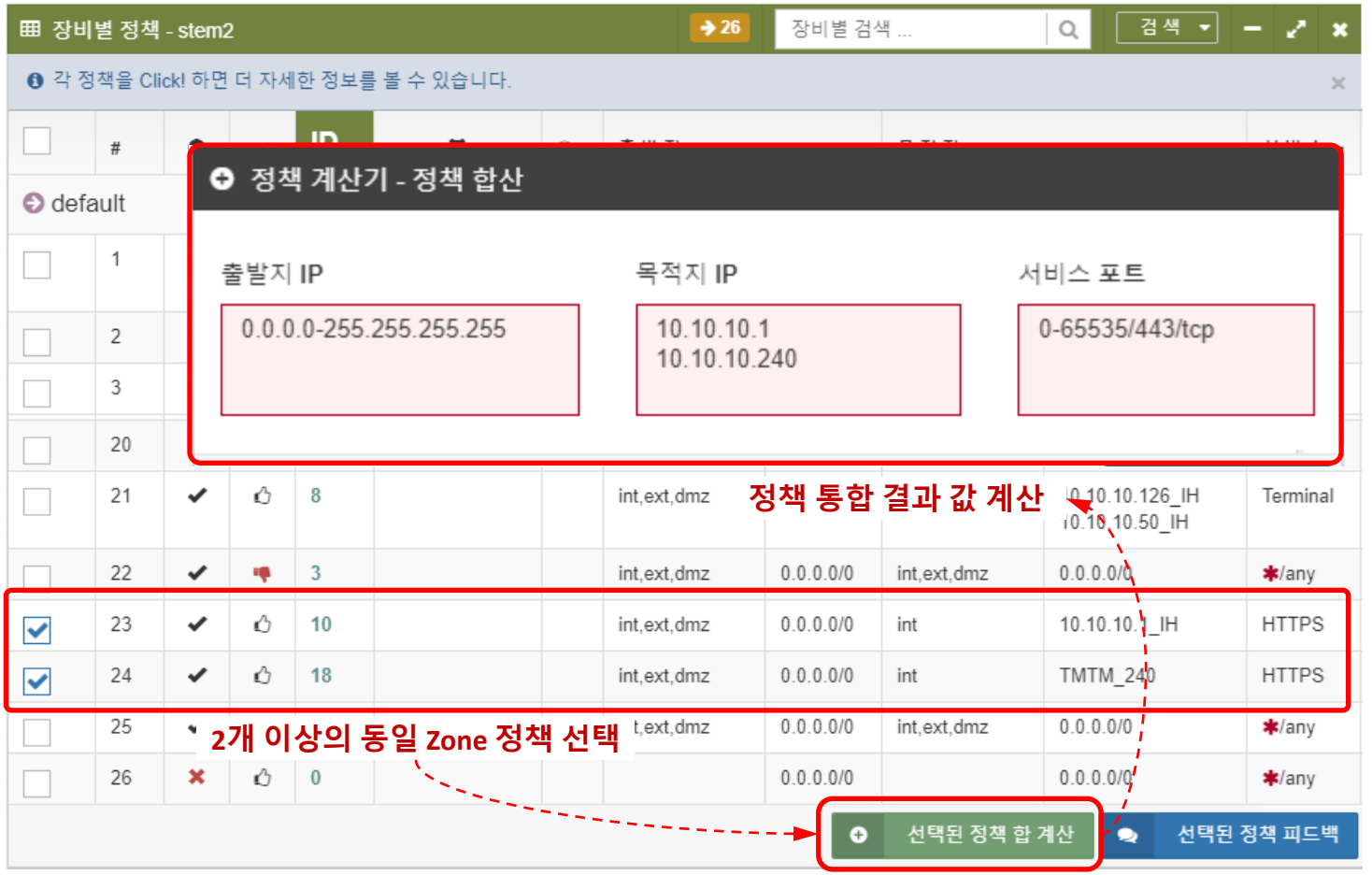



# 1. 스마트한『정책 최적화』기능

2개 이상의 정책을 통합한 결과값을 확인하는 기능으로, ① **통합 예정 정책 선택,** ② **정책 통합 결과 값 확인** 순서로 진행합니다.

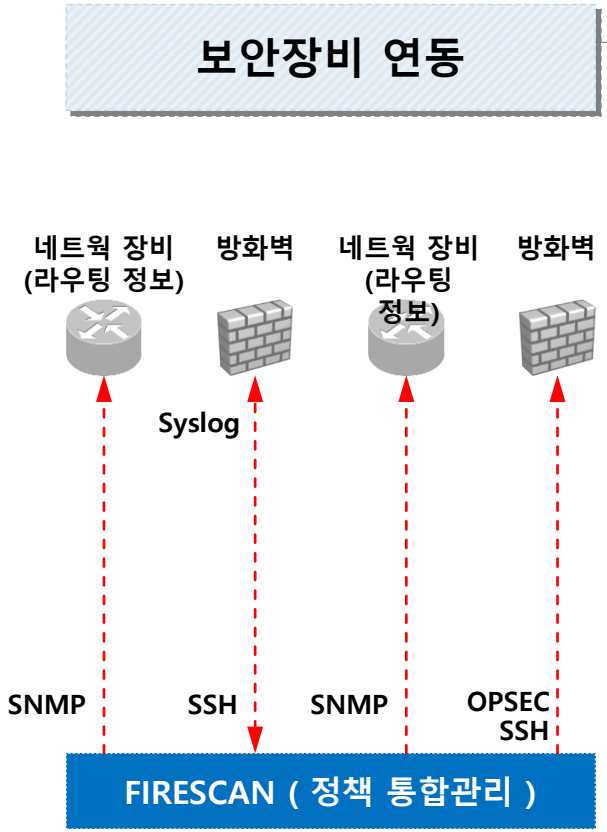
- 중복정책 분석
- 미사용 정책 분석
- 정책 순서 재배치
- 과다허용정책 실사용정책 분리제시
- 어플리케이션 객체 식별 및 중복 분석
- 정리대상 정책의 의견 일괄 취합
- **정책 통합**

• **2개 이상의 동일 Zone 정책을 통합한 결과 값 확인**



# 2. 장비 연동 및 네트워 토폴로지 맵 구성

## 『폭넓은 방화벽, 네트워크 장비 연동』 지원




### 방화벽 장비

- 정책/객체/Routing 정보 수집
  - Agentless 방식
- Syslog 수신
  - 실시간 로그 or 통합로그시스템 연동

### 네트워크 장비

- Routing 정보 수집
  - Agentless 방식
  - SNMP v1/v2/v3 지원

### 네트워크 토폴로지

- 자동 맵 구성
  - 경로 시뮬레이션 등 가시성 제공

### 방화벽 Health Check

- 사용률 모니터링
  - 임계치 초과 시, Alert

# 2. 장비 연동 및 네트워크 토폴로지 맵 구성

이기종 방화벽은 물론, **네트워크 장비의 보안정책**까지 통합 연동하여 관리해 줍니다.

**연동 장비 종류**

네트워크 토폴로지 맵

Health Check

- **국산, 외산 보안장비 차별 없이 모든 기능을 동일하게 지원**
- **신규 제조사의 보안장비도 빠른 연동이 가능**

| 국산 방화벽 | 지원 장비 |
|---|---|
| SECUI | • MF2, NXG  |
| AhnLab | • TrusGuard  |
| NexG | • NexG FW  |
| AXGATE Security and Beyond | • AXGATE  |
| FutureSystems | • WeGuardia  |

| 외산 방화벽 | 지원 장비 |
|---|---|
| Check Point SOFTWARE TECHNOLOGIES LTD. | • Check Point  |
| FORTINET | • FortiGate  |
| paloalto NETWORKS | • PA  |
| cisco | • ASA  |
| JUNIPER NETWORKS | • SRX, SSG, ISG  |

※ 어울림, 아이월 등의 국산 방화벽 연동 사례 있음

# 2. 장비 연동 및 네트워크 토폴로지 맵 구성

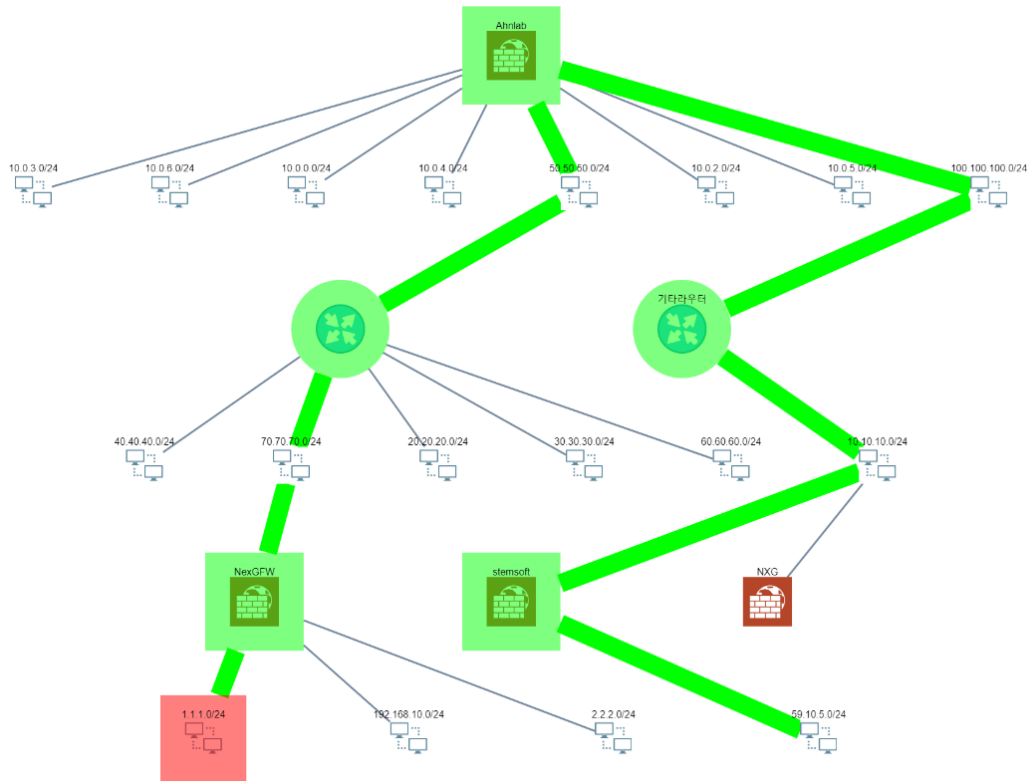
장비 등록만으로 네트워크 토폴로지 맵이 자동으로 그려집니다.

연동 장비 종류

**네트워크 토폴로지 맵**

Health Check

- **가상화 상태에서 시뮬레이션 된 경로를 맵 상에서 표시**
- **어떤 장비를 통하여 경로가 형성되었는지 직관적으로 확인 가능**
- **다양한 형태의 맵 알고리즘 제공**



# 2. 장비 연동 및 네트워크 토폴로지 맵 구성

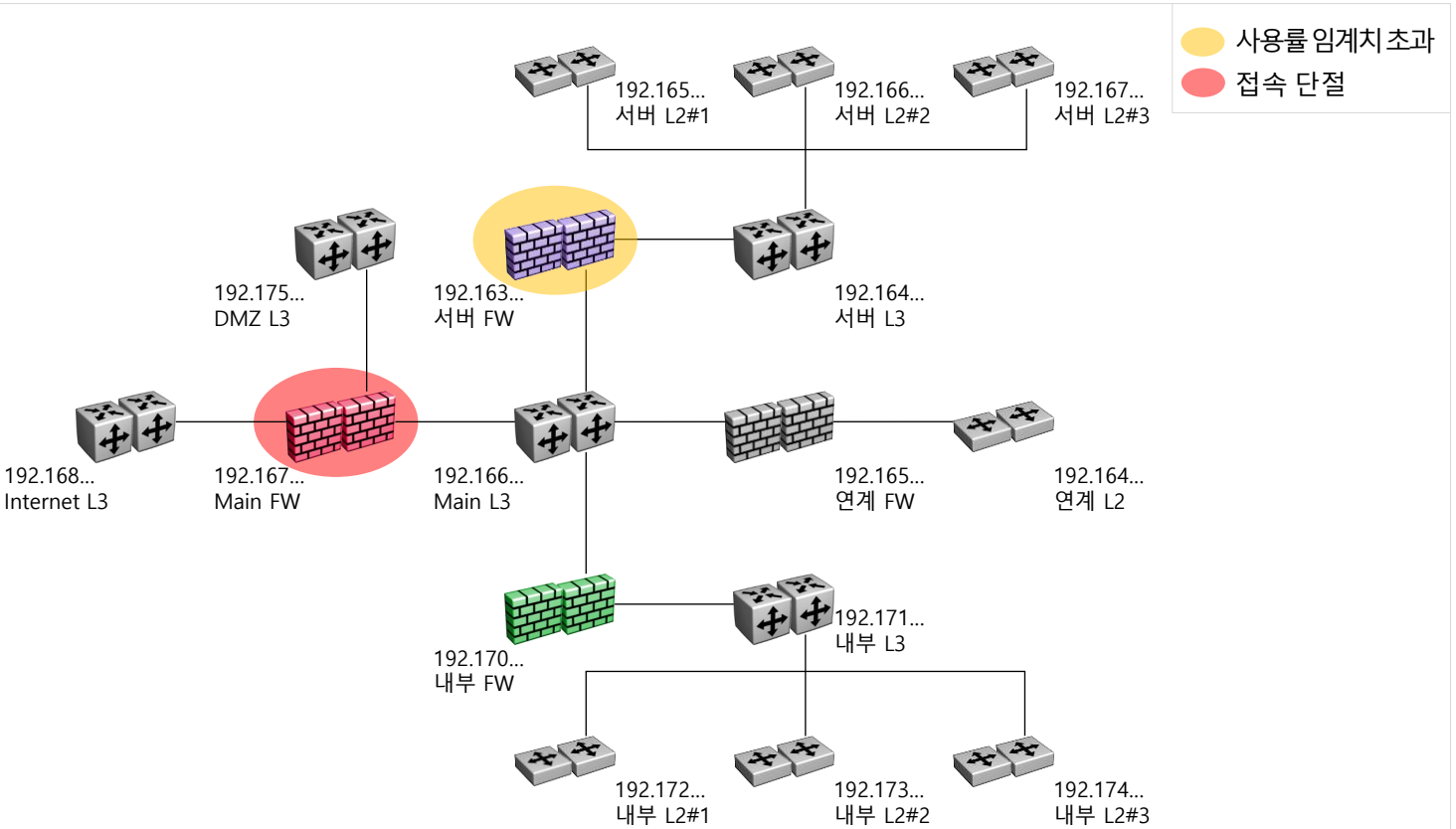
네트워크 토폴로지 맵의 각 노드는 활성화되어 있으며 장비의 이상유무가 표시됩니다.

연동 장비 종류

네트워크 토폴로지 맵

**Health Check**

- **관리대상 방화벽의 Alive 상태 표시**
- **설정된 임계치 기준으로 CPU/Memory/Disk 사용률 초과시 Alert 표시**



# 3. 편리한『사전 시뮬레이션』기능

## GUI 상에서 완전한『정책 What-If 분석』지원

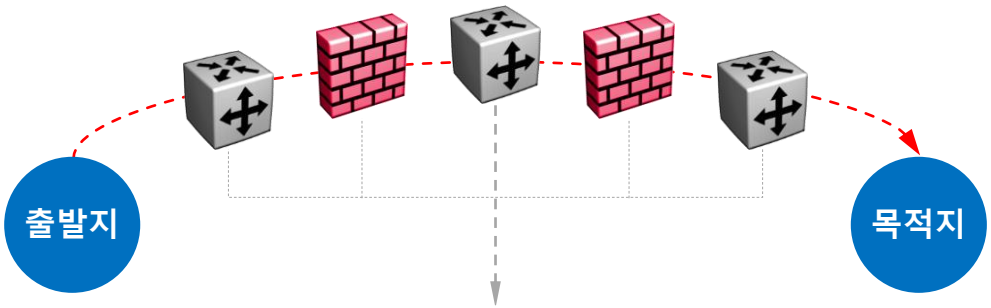
※ 정책 What-if 분석 : 가상 환경에서 적용 예정정책을 선 적용한 후 개통 예정업무의 정상 개통여부 사전 검증

**정책 사전 검증**

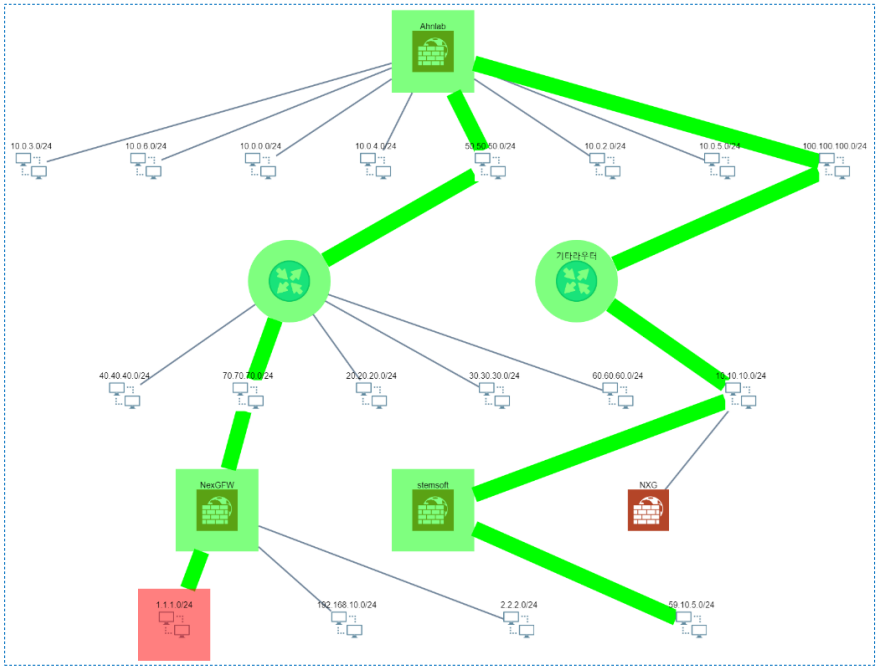
**What-If 시뮬레이션**

- 정책 검증
- 경로 탐색

- 경유 방화벽별 정책 허용여부 검증 (허용/차단)
- 자동 시각화 및 결과 표시




| 구분 | 결과 | 장비명 | 경유 네트워크 | 설명 |
|---|---|---|---|---|
| 경로 탐색 | | | 172.16.0.0/16 | 라우팅 테이블에 의한 경로 탐색 |
| 정책 검증 | 허용 | FW_DMZ | | 5번째 정책번호 '4'번에 의하여 통과 되었습니다. |
| 경로 탐색 | | | 10.10.8.0/24 | 라우팅 테이블에 의한 경로 탐색 |
| 정책 검증 | 허용 | FW_INT | | 11번째 정책번호 '8'번에 의하여 통과 되었습니다. |
| 경로 탐색 | | | 10.10.10.0/24 | 라우팅 테이블에 의한 경로 탐색 |



# 3. 편리한『사전 시뮬레이션』기능

적용예정 정책이 정상적으로 작동하는지에 대한 사전 검증은 ① **라우팅 경로의 존재**, ② **적용대상 방화벽**, ③ **정책적용의 정상 허용 여부**를 확인하는 것입니다.

**정책 가상 적용**

경로 시뮬레이션

## 적용 예정 정책

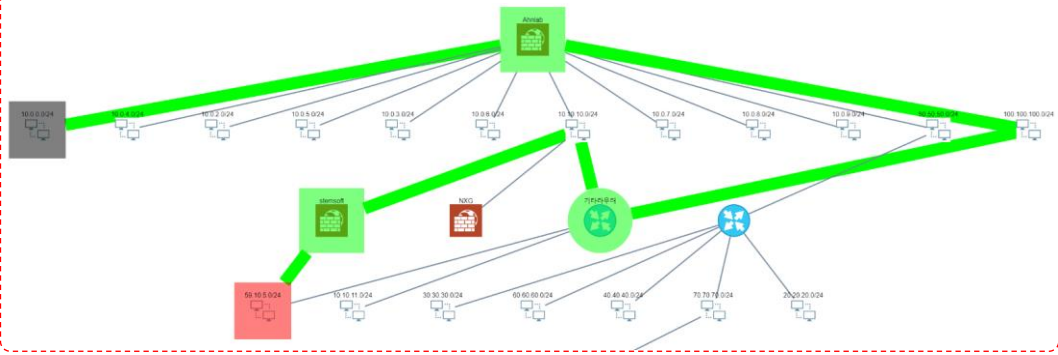
정책 What-If

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| ⊖ | Ahnlab | 정책추가 | 1 | 허용 | 10.0.0.1 | 59.10.5.1 | 80/tcp |

## 적용 예상 결과

경로

| # | 구 분 | 결 과 | 장 비 명 | 경유 네트워크 | 설 명 |
|---|---|---|---|---|---|
| 1 | 경로 탐색 | | Ahnlab | 10.0.0.0/24 | 라우팅 테이블에 의한 경로 탐색 |
| 2 | 정책 검증 | ✔ 허용 | Ahnlab | | 1번째 정책번호 "TEST"에 의하여 통과 되었습니다. |
| 3 | 경로 탐색 | | Ahnlab | 100.100.100.0/24 | 라우팅 테이블에 의한 경로 탐색 |
| 4 | 경로 탐색 | | 기타라우터 | 100.100.100.0/24 | 라우팅 테이블에 의한 경로 탐색 |
| 5 | 경로 탐색 | | 기타라우터 | 10.10.10.0/24 | 라우팅 테이블에 의한 경로 탐색 |
| 6 | 경로 탐색 | | stemsoft | 10.10.10.0/24 | 라우팅 테이블에 의한 경로 탐색 |
| 7 | 정책 검증 | ✔ 허용 | stemsoft | | 41번째 정책번호 "30"에 의하여 통과 되었습니다. |
| 8 | 경로 탐색 | | stemsoft | 59.10.5.0/24 | 라우팅 테이블에 의한 경로 탐색 |



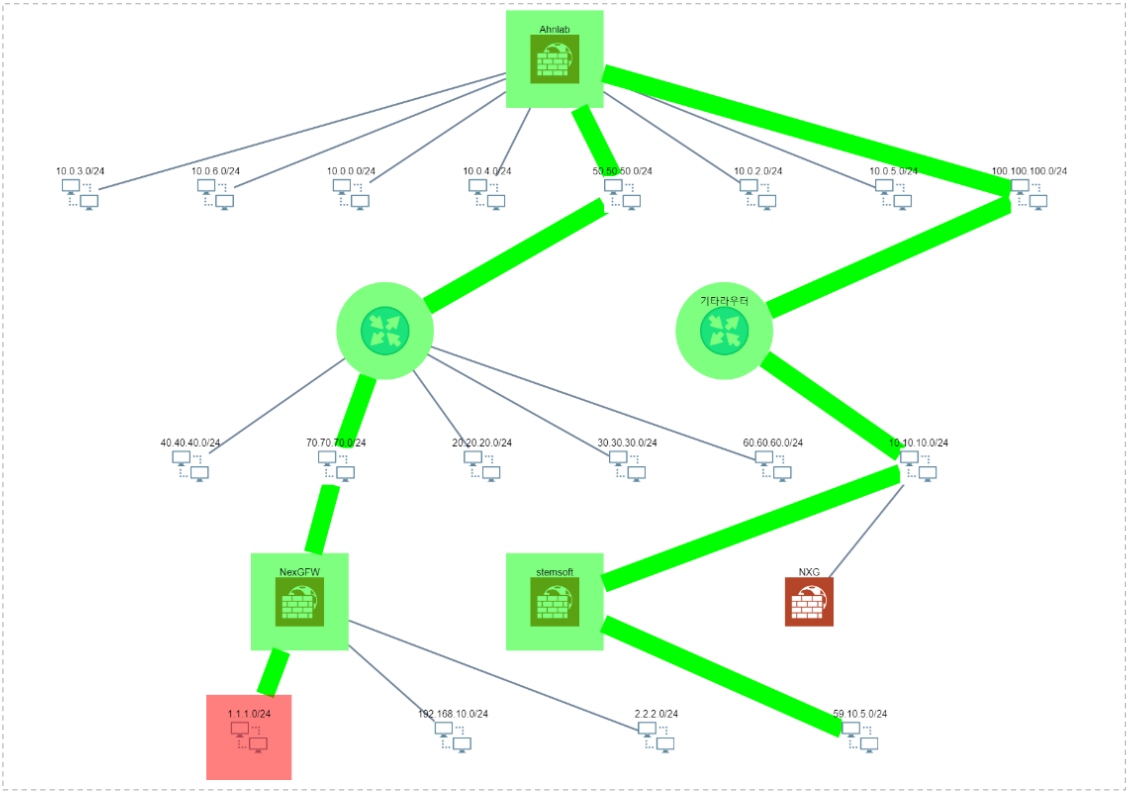
# 3. 편리한『사전 시뮬레이션』기능

분석 버튼을 클릭하면 네트워크 토폴로지 맵과 테이블 상에 경로와 허용/차단 유무, 그리고 통과된 정책 ID가 표시됩니다.

정책 가상 적용

**경로 시뮬레이션**

| 구분 | 결과 | 장비명 | 경유 네트워크 | 설명 |
|---|---|---|---|---|
| 경로 탐색 | | | 172.16.0.0/16 | 라우팅 테이블에 의한 경로 탐색 |
| 정책 검증 | 허용 | FW_DMZ | | 5번째 정책번호 '4'번에 의하여 통과 되었습니다. |
| 경로 탐색 | | | 10.10.8.0/24 | 라우팅 테이블에 의한 경로 탐색 |
| 정책 검증 | 허용 | FW_INT | | 11번째 정책번호 '8'번에 의하여 통과 되었습니다. |
| 경로 탐색 | | | 10.10.10.0/24 | 라우팅 테이블에 의한 경로 탐색 |



# 4. 유용한『정책 현황 분석』기능

## 사용자 편의 지향『정책 현황 분석』기능

**정책 현황 분석**

- **만료예정정책**
  - 시간객체 자동 로딩 — ▪ 방화벽에서 정책 만료일 자동 로딩
  - 담당자 사전 통보 — ▪ 내부 메일시스템, SMS 연동 지원
- **정책 이력 관리**
  - 정책 비교 — ▪ 동일 or 이기종 방화벽 정책 버전간 비교
  - 변경 내역 관리 — ▪ 기간별 정책 변경내역 조회
- **위험 분석**
  - 과다허용 정책 등 분석 — ▪ Any or Class 단위 과다허용 정책 분석
- **컴플라이언스 검증**
  - PCI-DSS, ISMS 등 규정 위반 — ▪ 즉각적 위험 분석
  - 사용자 정의 규정 위반 — ▪ 내부규정 정의 및 맞춤형 분석
- **정책 모니터링**
  - 중요한 정책 변경 모니터링 — ▪ 주요 서비스 실시간 모니터링

# 4. 유용한『정책 현황 분석』기능

만료예정정책을 달력 형태로 편리하게 조회할 수 있도록 지원합니다.

**만료예정정책 관리**

정책 비교

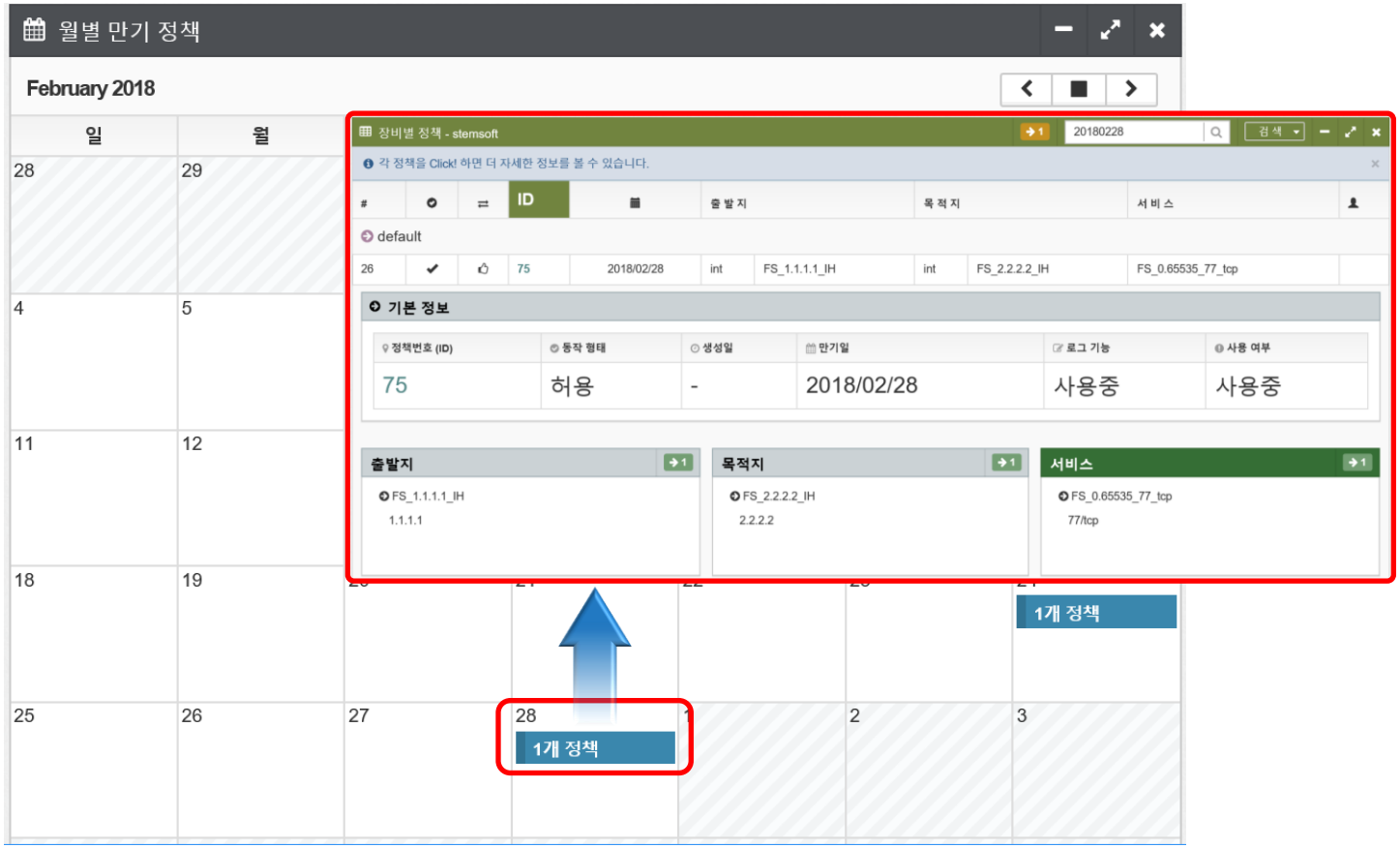
정책 변경내역 관리

위험 분석

컴플라이언스 검증

정책 모니터링

- **시간 객체를 자동 분석하여 관리자가 쉽게 인지할 수 있도록 화면 구성**
- **모든 정책 만료를 쉽게 검색**

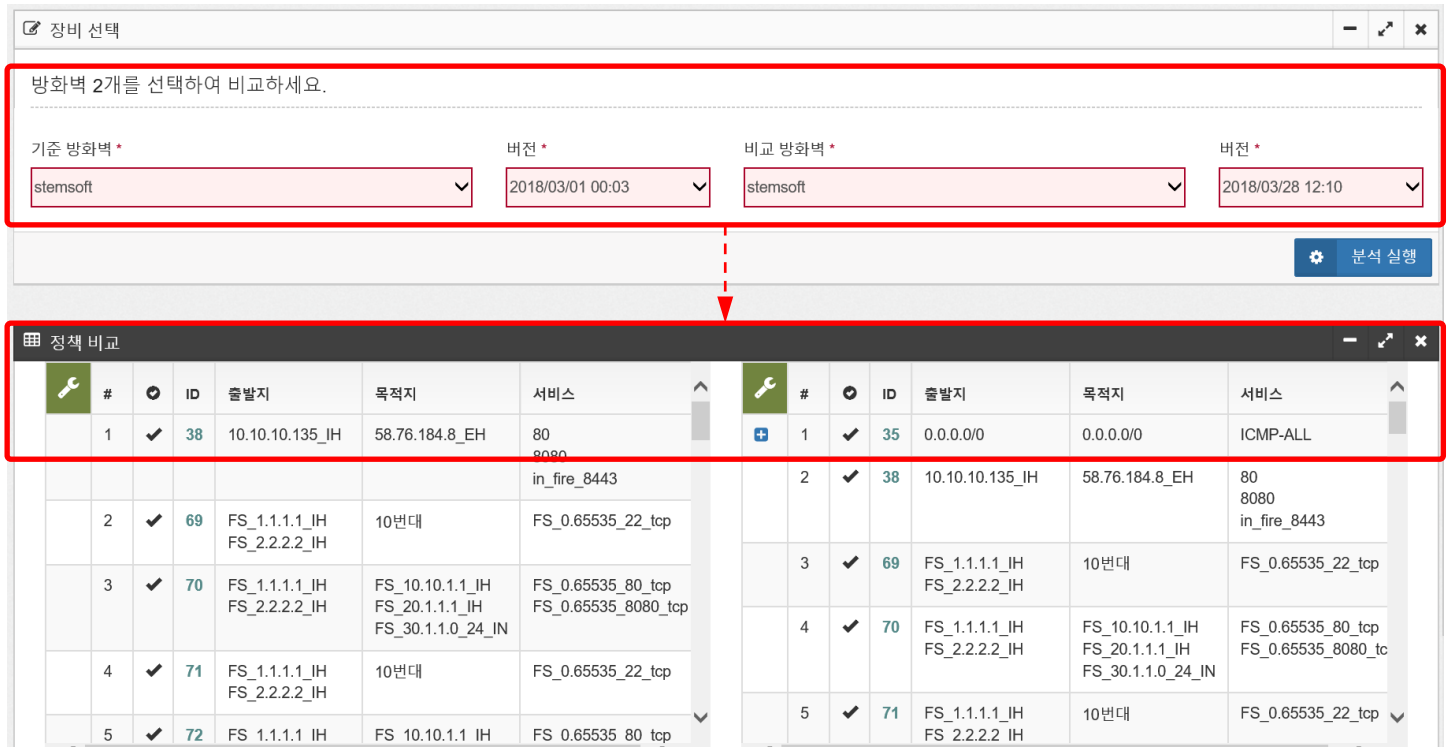


# 4. 유용한『정책 현황 분석』기능

동일 장비 혹은 이기종 장비 간의 정책을 서로 비교하여 차이점을 분석합니다.

- 만료예정정책 관리
- **정책 비교**
- 정책 변경내역 관리
- 위험 분석
- 컴플라이언스 검증
- 정책 모니터링

- **(동일 장비) 어떤 정책이 추가, 수정, 삭제되었는지 쉽게 확인 가능**
- **(이기종 장비) 장비간 설정 정책 비교**

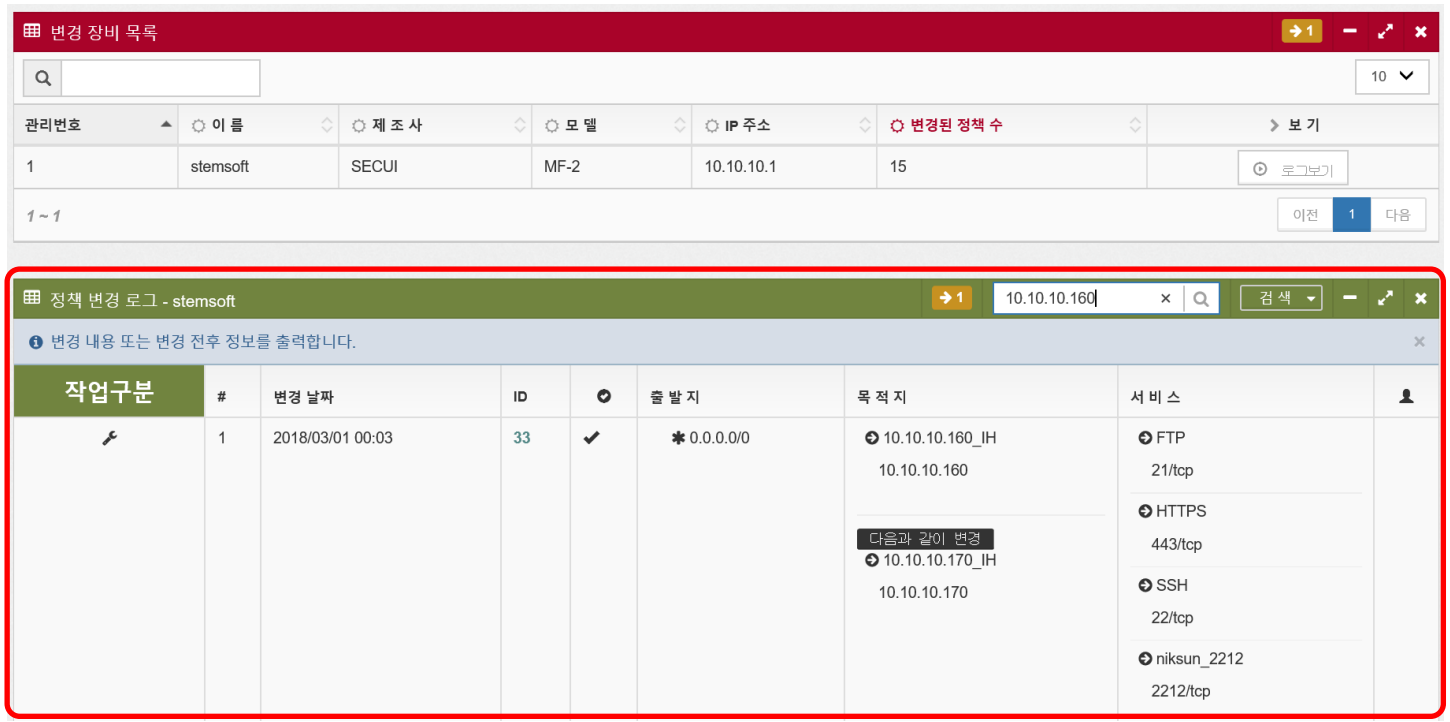


# 4. 유용한『정책 현황 분석』기능

동일 장비 혹은 이기종 장비 간의 정책을 서로 비교하여 차이점을 분석합니다.

- 만료예정정책 관리
- 정책 비교
- **정책 변경내역 관리**
- 위험 분석
- 컴플라이언스 검증
- 정책 모니터링

- **정책의 추가, 삭제, 수정 등 정책의 변경을 관리**
- **관리자 설정 등을 추적하여 변경 내용 저장**

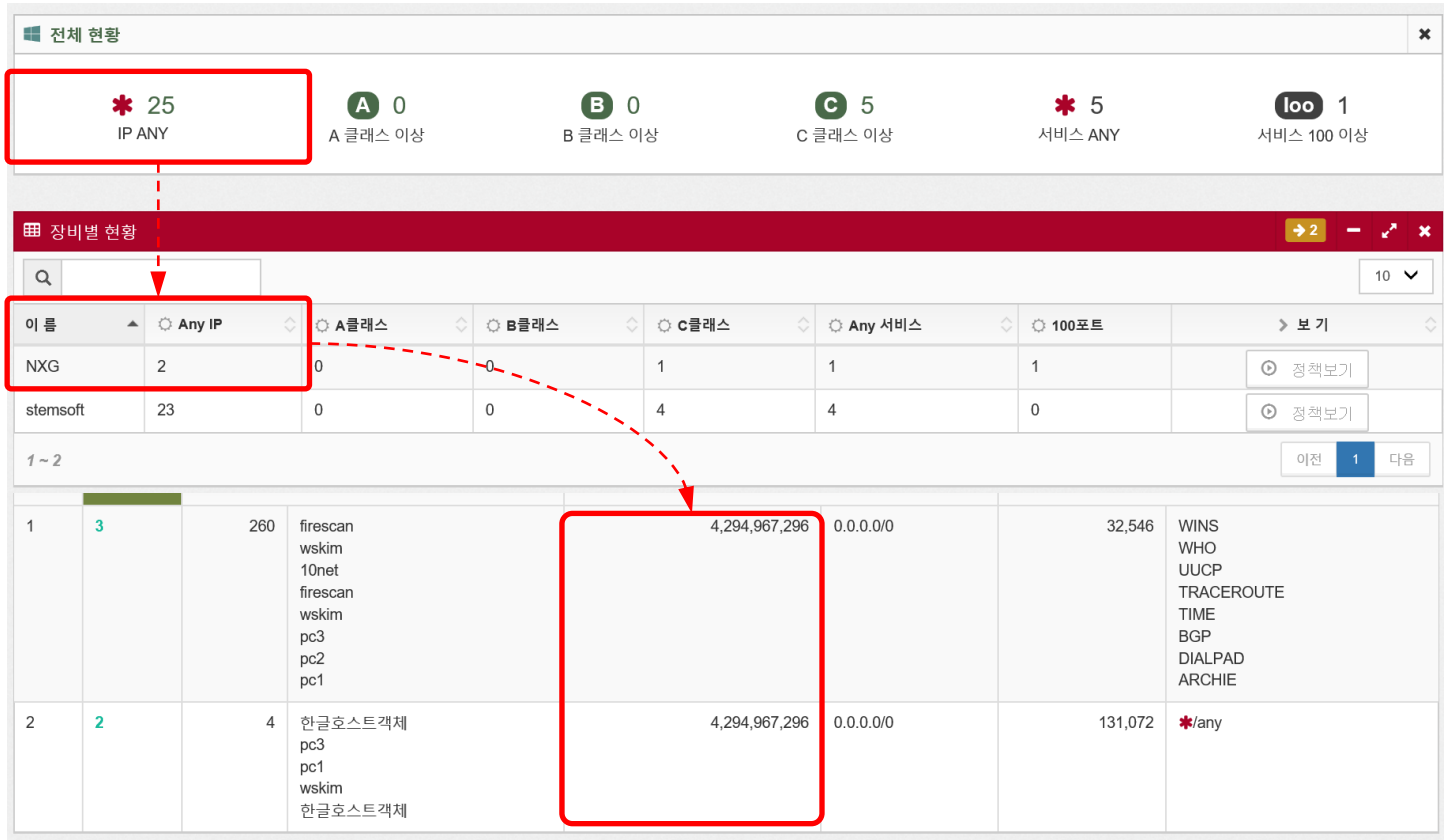


# 4. 유용한『정책 현황 분석』기능

위험 분석기능 중의 하나로 과다허용 정책에 대한 상세 분석기능을 제공합니다.

- 만료예정정책 관리
- 정책 비교
- 정책 변경내역 관리
- **위험 분석**
- 컴플라이언스 검증
- 정책 모니터링

- **방화벽 정책 중, 과도하게 열린 IP주소 및 서비스에 대한 분석**
  - ✓ Any 오픈 정책
  - ✓ A,B,C Class 오픈 정책

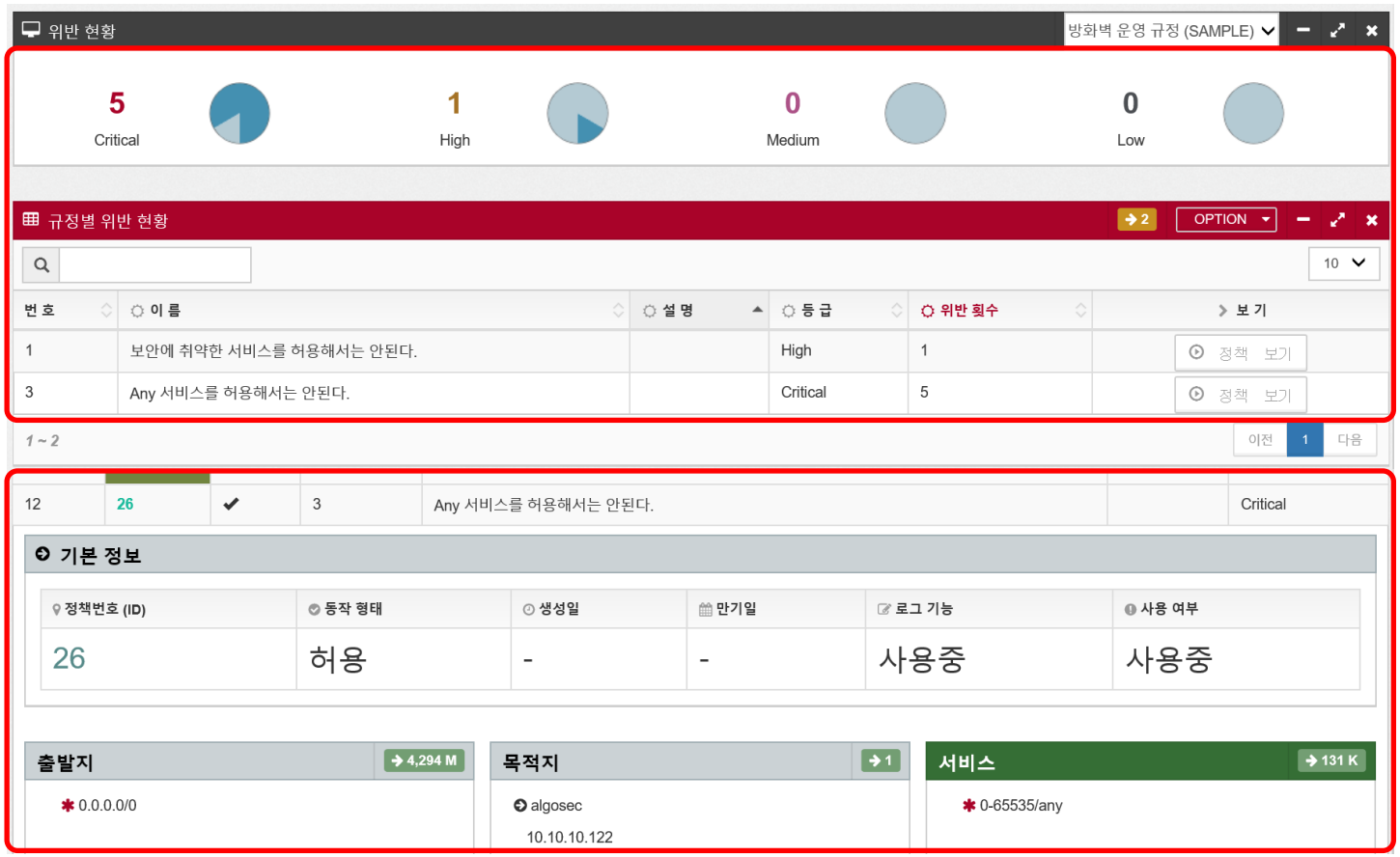


# 4. 유용한『정책 현황 분석』기능

표준 보안 템플릿 및 고객사 보안 규정에 따른 보안 컴플라이언스 커스터마이징을 제공합니다.

- 만료예정정책 관리
- 정책 비교
- 정책 변경내역 관리
- 위험 분석
- **컴플라이언스 검증**
- 정책 모니터링

- **국제적으로 널리 통용되는 PCI DSS, ISMS, 자체 샘플 내장**
- **내부 방화벽 규정 등록 후, 위반 여부 분석**



# 4. 유용한『정책 현황 분석』기능

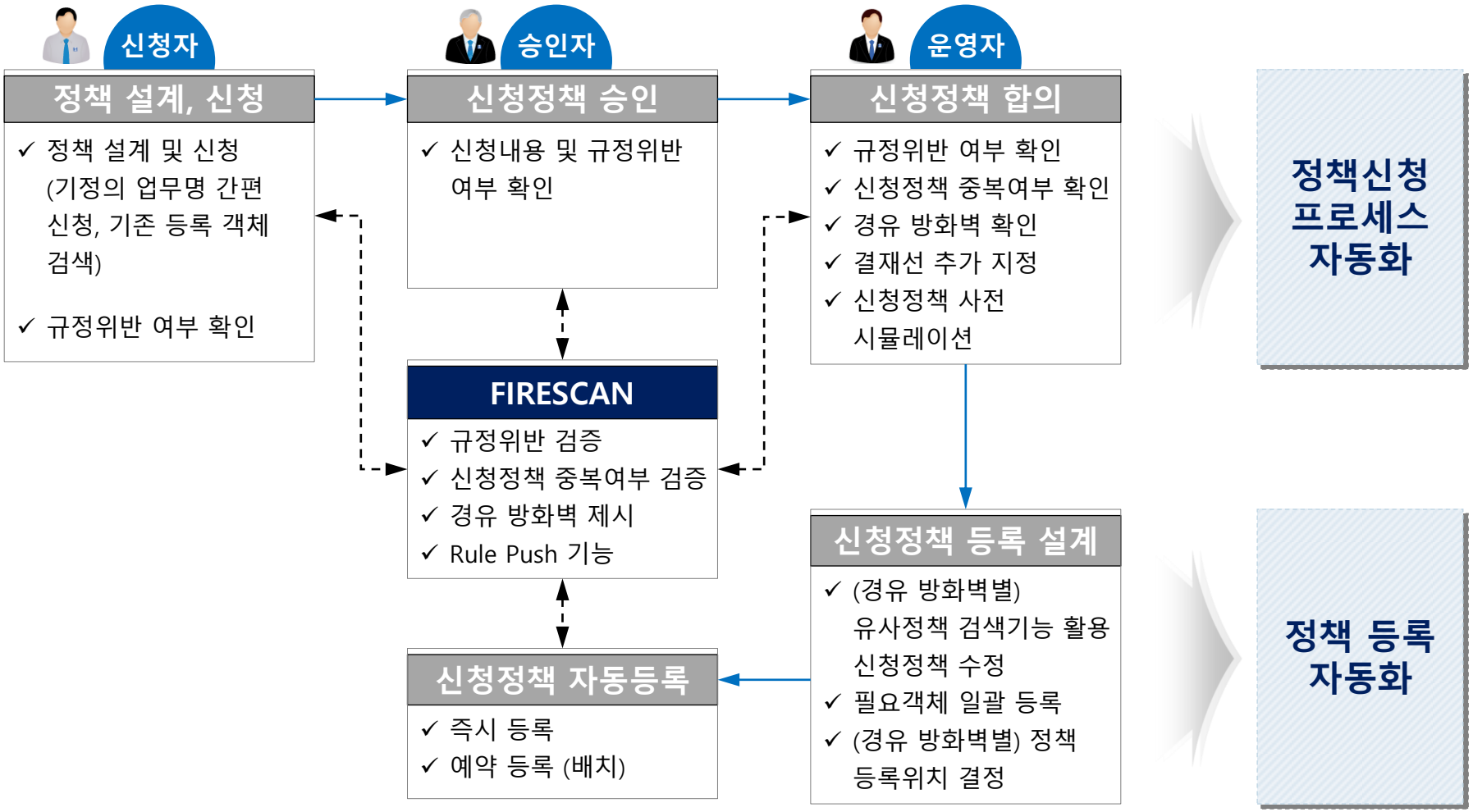
중요한 방화벽 정책에 대한 실시간 모니터링을 제공합니다.

- 만료예정정책 관리
- 정책 비교
- 정책 변경내역 관리
- 위험 분석
- 컴플라이언스 검증
- **정책 모니터링**

• **주요 서비스에 대한 실시간 모니터링**

# 5. 유연한『방화벽 정책신청 관리시스템』

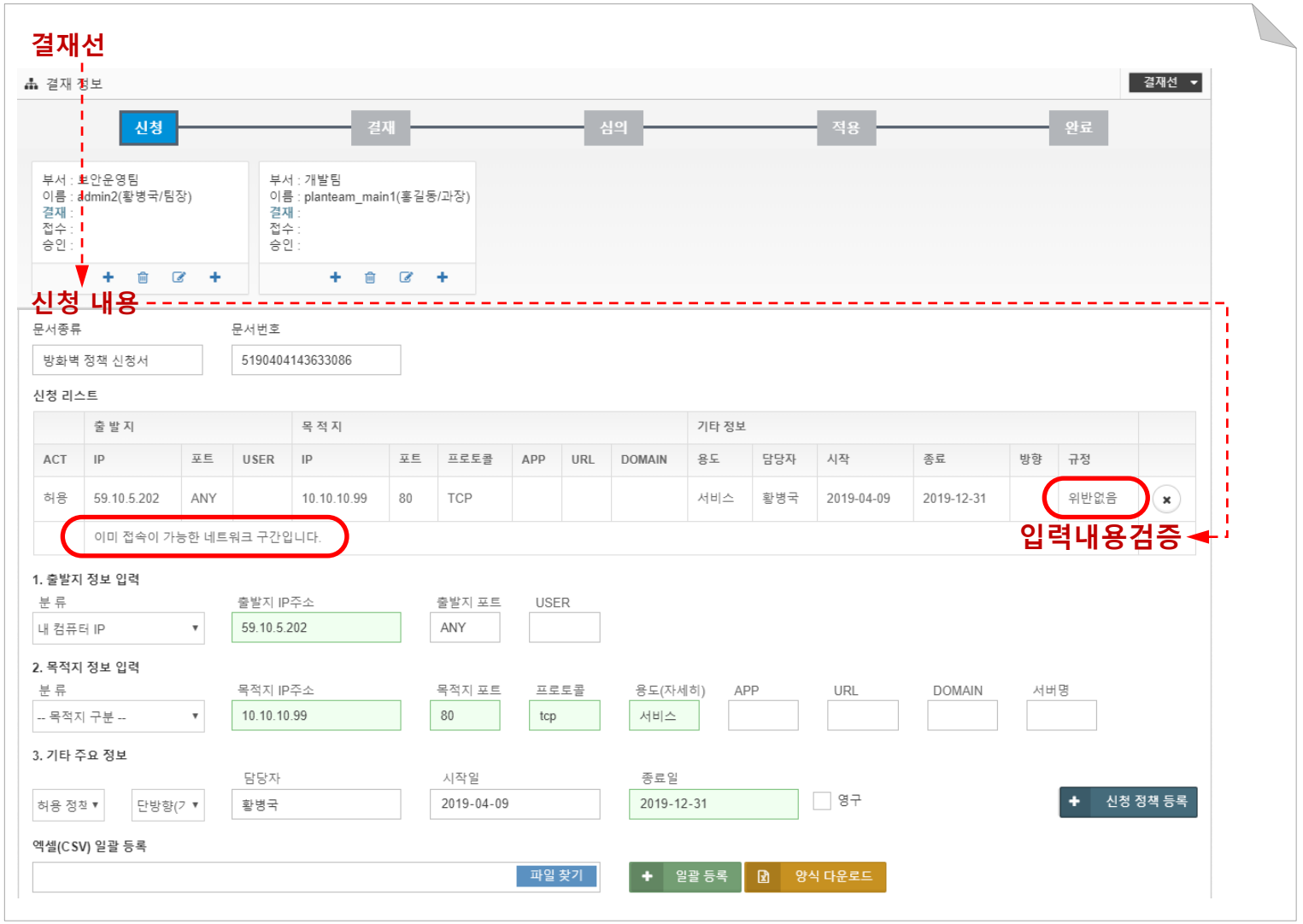
## 『방화벽 정책신청 관리시스템』의 고객 맞춤형 구성 및 연계기능 지원



# 5. 유연한『방화벽 정책 신청 시스템』

정책 신청자는 ① **정책신청**, ② **입력내용검증(위험분석, 규정위반검증, 중복검사)**, ③ **결재선 지정** 순서로 정책을 신청합니다.

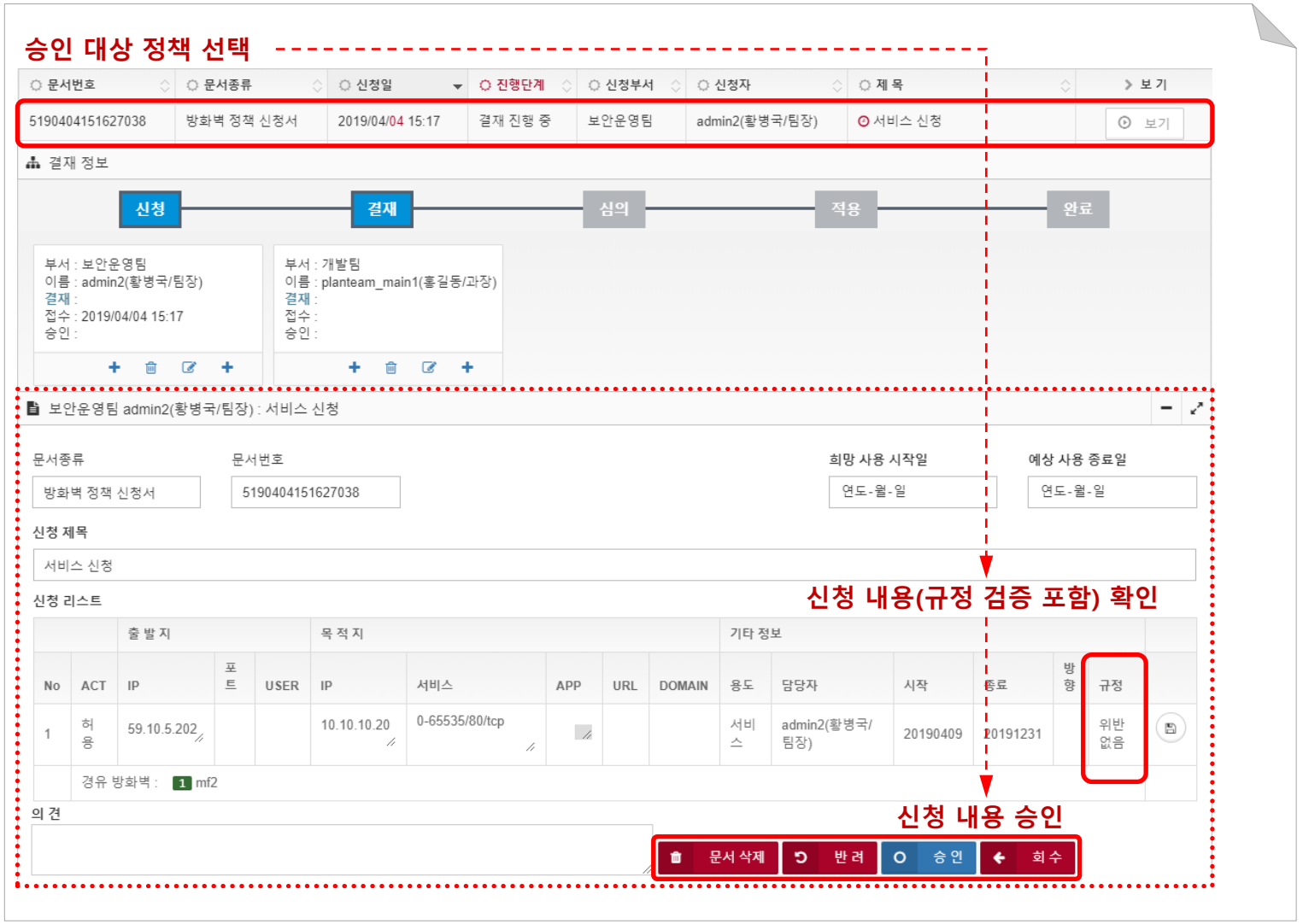
- **정책 신청**
- 신청정책 승인
- 신청정책 합의
- 정책 시뮬레이션
- 경로 시뮬레이션
- 방화벽 Rule Push



# 5. 유연한『방화벽 정책 신청 시스템』

정책 신청자는 ① **정책신청**, ② **입력내용검증(위험분석, 규정위반검증, 중복검사)**, ③ **결재선 지정** 순서로 정책을 신청합니다.

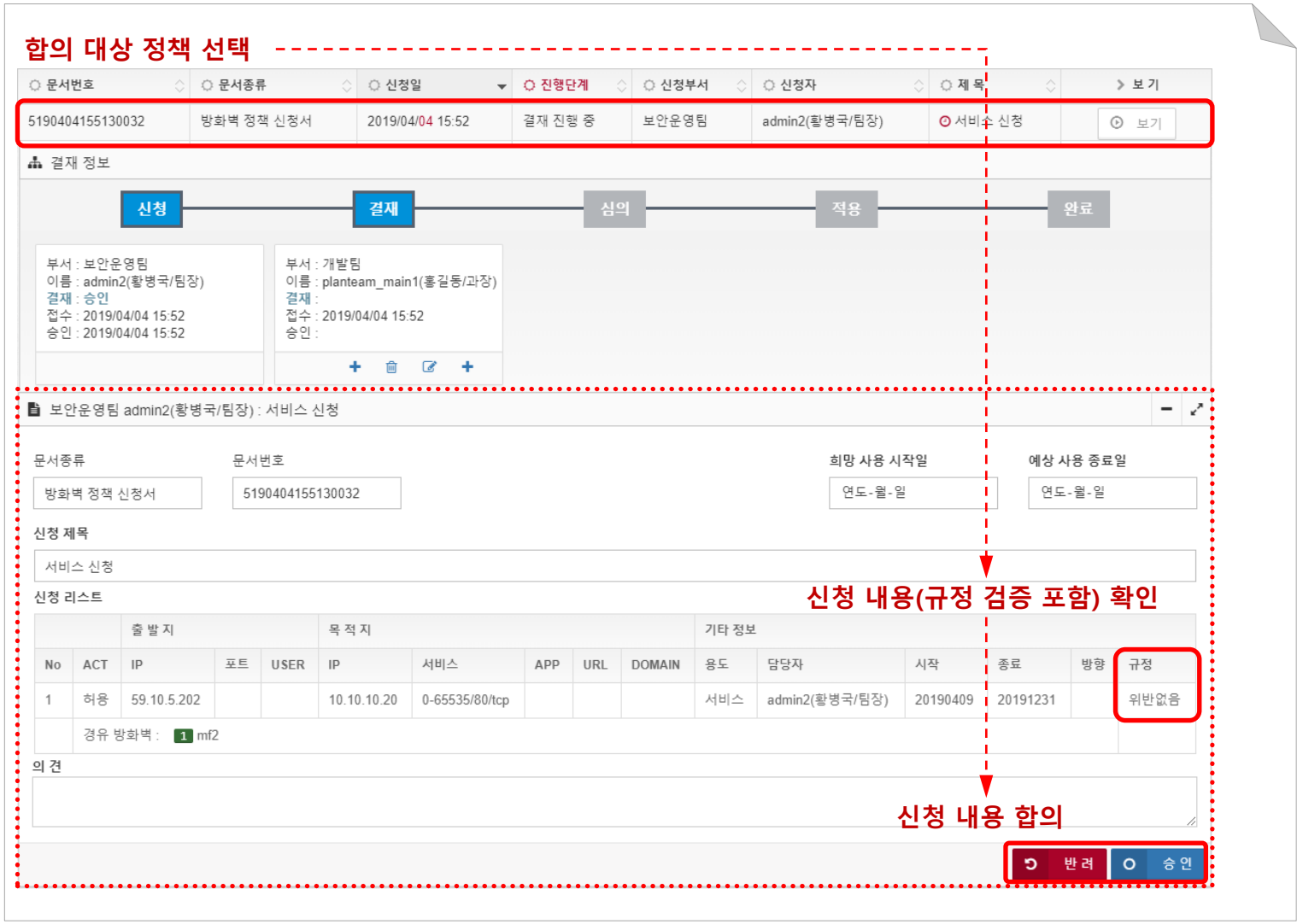
- 정책 신청
- **신청정책 승인**
- 신청정책 합의
- 정책 시뮬레이션
- 경로 시뮬레이션
- 방화벽 Rule Push



# 5. 유연한『방화벽 정책 신청 시스템』

방화벽 운영부서에서는 신청된 정책들을 확인한 후 적용여부를 결정(합의/반려)합니다.

- 정책 신청
- 신청정책 승인
- **신청정책 합의**
- 정책 시뮬레이션
- 경로 시뮬레이션
- 방화벽 Rule Push





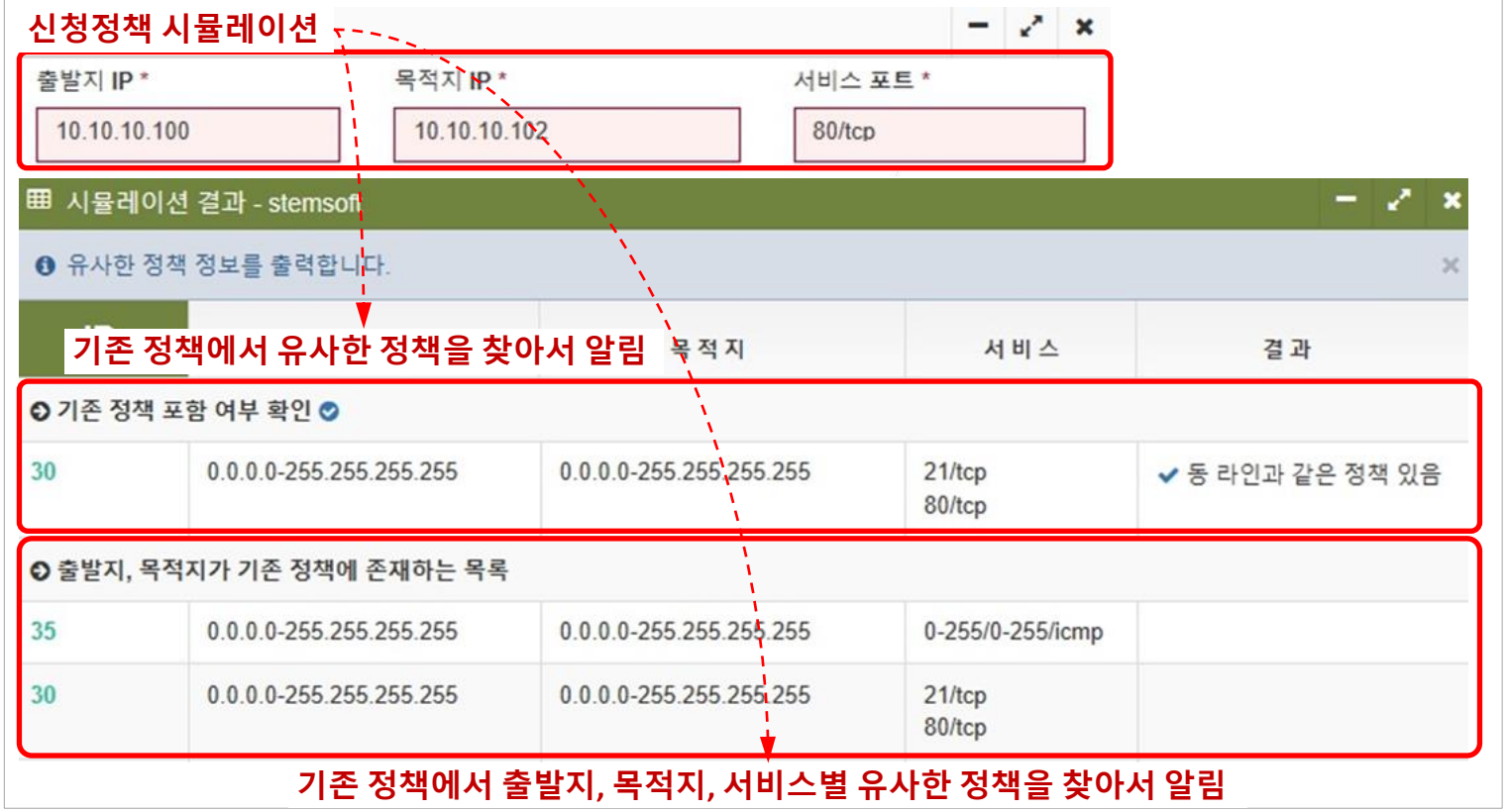

JMTRUE (주)제이엠트루

# 5. 유연한『방화벽 정책 신청 시스템』

정책 시뮬레이션을 통해 신청된 정책에 대한 동일정책의 기 존재 유무, 기존 정책을 확장하여 적용하는 방법 등을 안내 받을 수 있습니다.


정책 신청
신청정책 승인
신청정책 합의
정책 시뮬레이션
경로 시뮬레이션
방화벽 Rule Push


- **방화벽 정책을 추가하기 전, 가상화 상태에서 정책 적용 테스트 수행**
  - ✓ 이미 정책이 존재하는지 여부
  - ✓ 기존 정책에서 유사한 정책을 찾아서 알림
  - ✓ 출발지, 목적지, 서비스 별 일부 중복 정책, 기존 정책에 연속하여 적용 가능 여부






JMTRUE (주)제이엠트루

# 5. 유연한『방화벽 정책 신청 시스템』

적용 정책의 ① **라우팅 경로의 존재, ② 적용대상 방화벽, ③ 입력정책의 정상 허용 여부**를 가상의 환경에서 확인합니다.


정책 신청

신청정책 승인

신청정책 합의

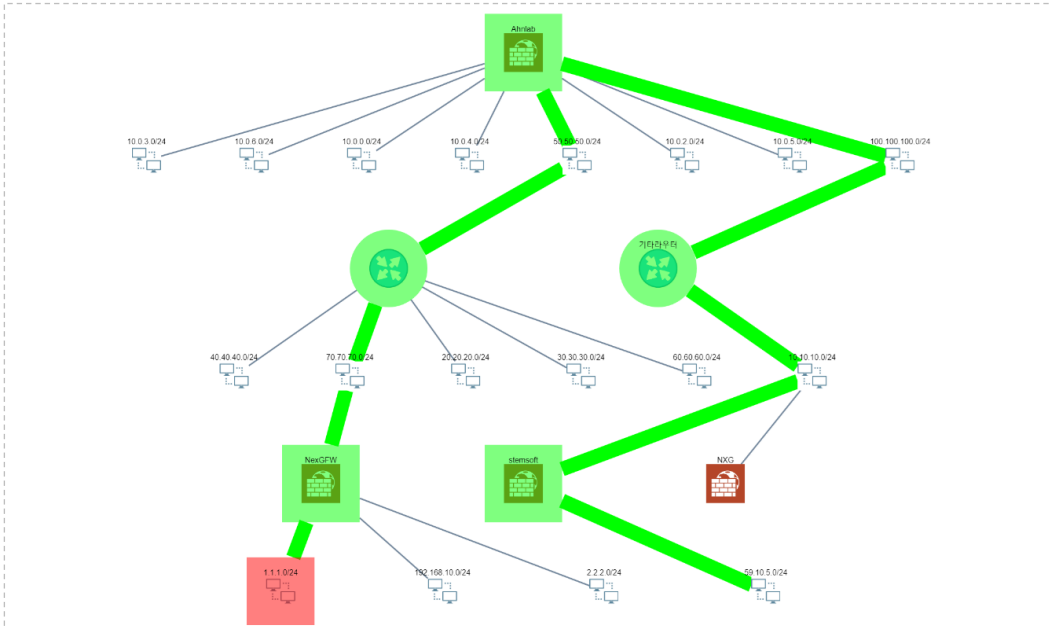
정책 시뮬레이션

**경로 시뮬레이션**

방화벽 Rule Push


- **장비 라우팅 및 NAT 정보, 장비 구성정보를 가상 환경에서 경로 시뮬레이션 지원**
  - ✓ 주어진 정책에 대해 경유 방화벽을 탐색
  - ✓ 경유 방화벽별로 허용/차단 상태 확인

| 구분 | 결과 | 장비명 | 경유 네트워크 | 설명 |
|---|---|---|---|---|
| 경로 탐색 | | | 172.16.0.0/16 | 라우팅 테이블에 의한 경로 탐색 |
| 정책 검증 | 허용 | FW_DMZ | | 5번째 정책번호 '4'번에 의하여 통과 되었습니다. |
| 경로 탐색 | | | 10.10.8.0/24 | 라우팅 테이블에 의한 경로 탐색 |
| 정책 검증 | 허용 | FW_INT | | 11번째 정책번호 '8'번에 의하여 통과 되었습니다. |
| 경로 탐색 | | | 10.10.10.0/24 | 라우팅 테이블에 의한 경로 탐색 |






JMTRUE (주)제이엠트루

# 5. 유연한『방화벽 정책 신청 시스템』

적용 정책의 ① **경유 방화벽,** ② **적용대상 위치,** ③ **수행 방법(예약, 즉시)** 을 지정합니다.

정책 신청

신청정책 승인

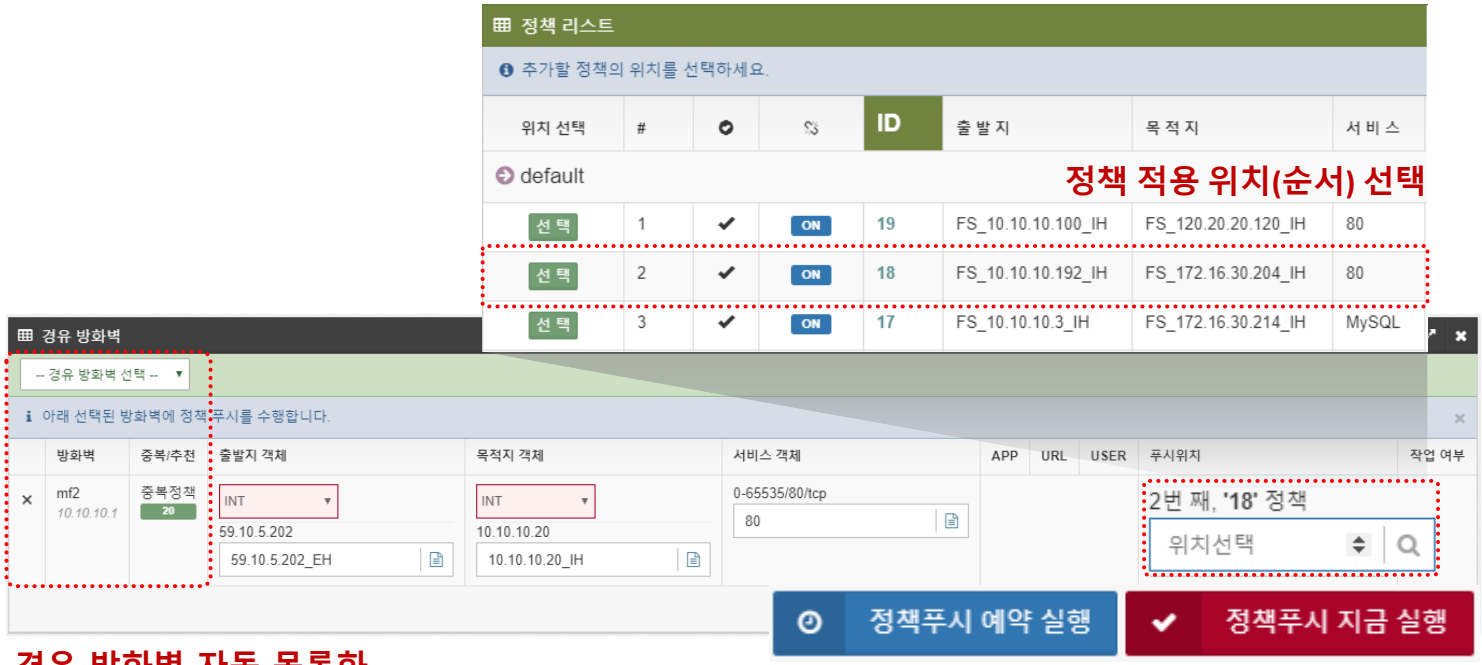
신청정책 합의

정책 시뮬레이션

경로 시뮬레이션

**방화벽 Rule Push**

- **실제 장비에 신청한 방화벽 정책을 적용**
  - ✓ 주어진 정책에 대해 경유 방화벽을 탐색
  - ✓ 적용할 위치(순서) 및 적용 방법(예약, 즉시) 선택



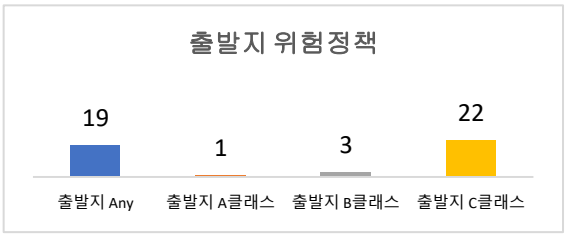
# 6. 시각화된 보고서 지원

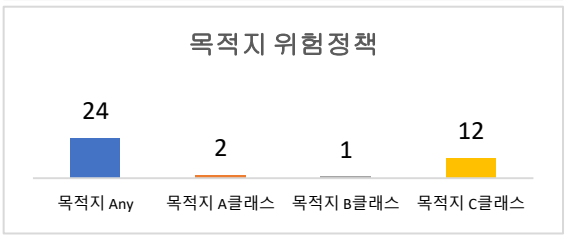
## 보고서 지원

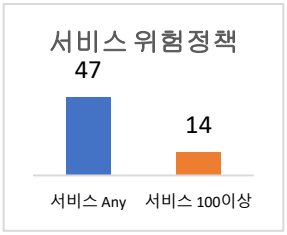
### 시각적 보고서

**가독성, 가시성 향상**

- **집계표, 그래프**
  - 고객 요구사항을 적극적으로 수용
- **구성**
  - 장비별 보고서, 통합 보고서 지원




| 서비스 Any | 서비스 100이상 |
|---|---|
| 47 | 14 |

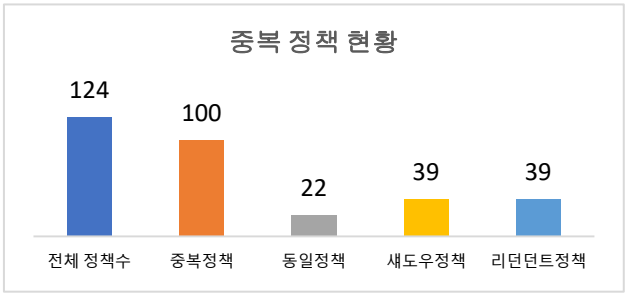
- 방화벽 ACL정책 리스트 보고서
- 전체 방화벽을 대상으로 한 정책 만기일 보고서
- 중복된 정책 리스트 보고서
- 과다하게 열린 출발지/목적지/서비스 정책 리스트 보고서
- 방화벽 ACL 정책 사용 현황 보고서
- 방화벽 정책 변경 이력 현황 보고서
- 전체 규정 위반 통계 보고서
- 방화벽 규정 위반 리스트 보고서
- 등록된 전체 장비 현황 보고서
- 방화벽 정책 재배치 제안 보고서
- 방화벽 정책 집중 분석 및 정책 제안 보고서
- 방화벽 1대 종합 정책 보고서
- 방화벽 NAT정책 리스트 보고서
- 전체 방화벽 중복 정책 현황 보고서
- 전체 방화벽 과도하게 열린 위험정책 현황 보고서
- 전체 방화벽 정책 변경 이력 현황 보고서

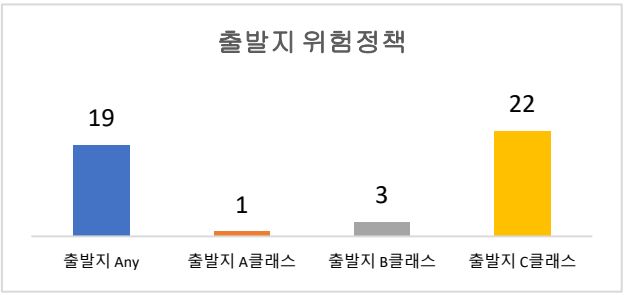
# 6. 시각화된 보고서 지원

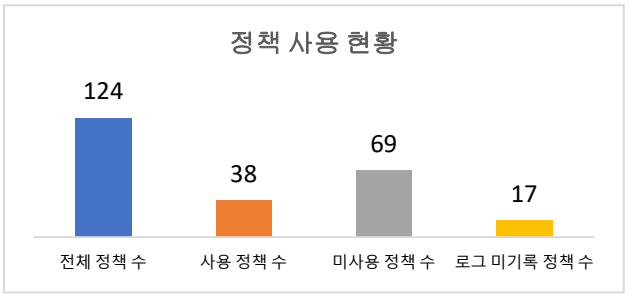
한눈에 알아보기 쉽게 시각화되고 테이블화된 형태의 보고서를 제공합니다.

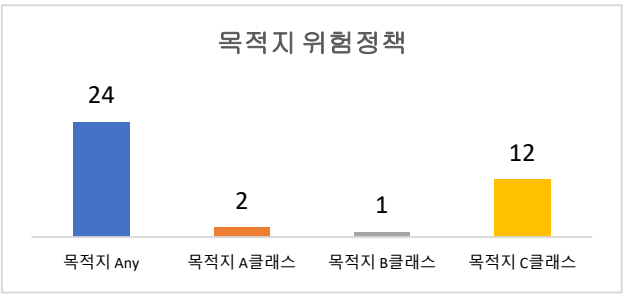
## 보고서 스타일

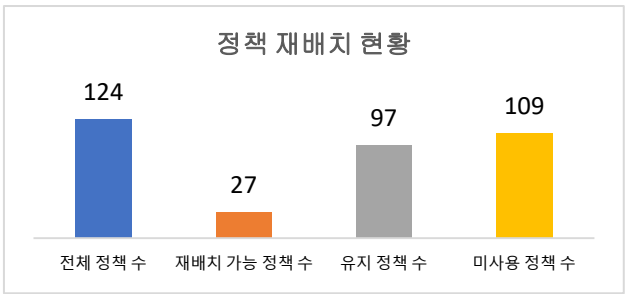
- **분석 항목별, 통합 보고서 제공**
- **엑셀, XML 형식 저장 기능**

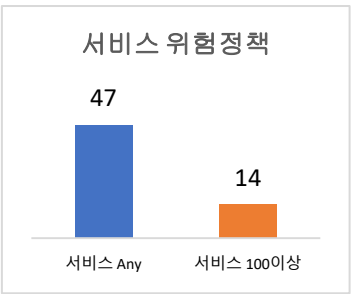



| 서비스 Any | 서비스 100이상 |
|---|---|
| 47 | 14 |

# III. FIRESCAN 구성 및 사양

1. 시스템 구성

2. 제품 사양
   1) Manager, Collector, Flow Manager, Analyzer

3. 인증
   1) GS인증 1등급 제품
   2) 조달등록제품

4. Reference
   1) 구축
   2) 정책 최적화 컨설팅

JMTRUE
(주)제이엠트루

# 1. 시스템 구성

방화벽 운영자

정책 담당자

FIRESCAN Manager

FIRESCAN Flow Manager

FIRESCAN Collector

Firewall, Network Switch

**방화벽 운영자**
- Manager/Flow Manager 접속

**정책 담당자**
- Flow Manager 접속

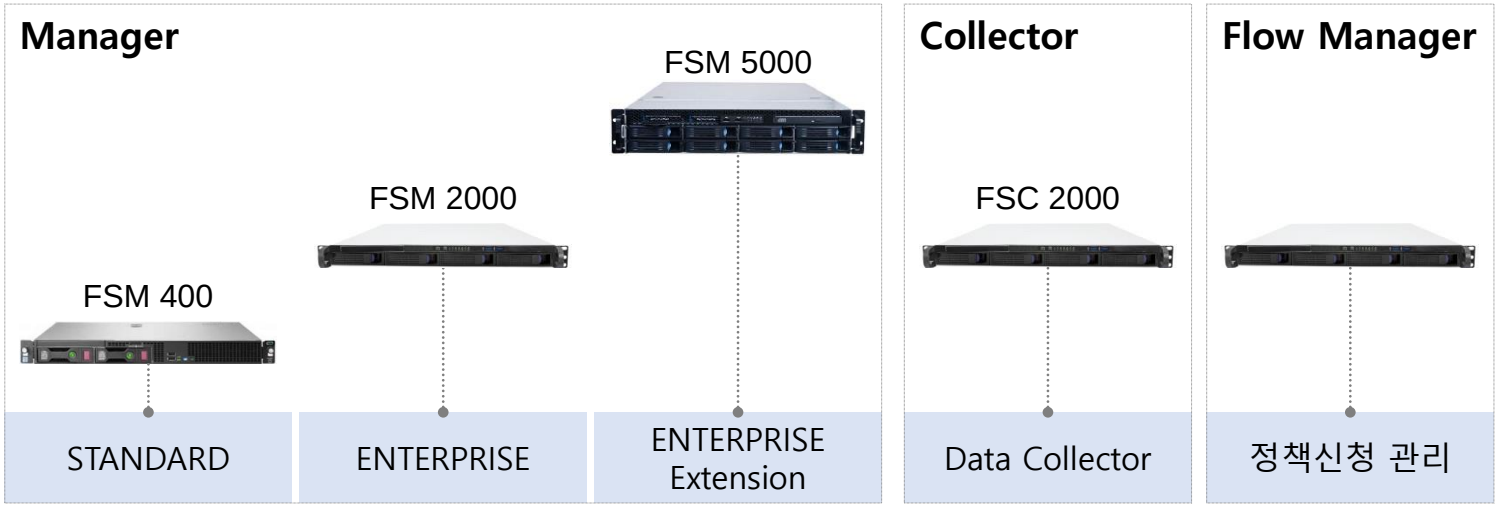
**FIRESCAN Manager**
- 방화벽 데이터 분석, 최적화, 통합관리

**FIRESCAN Flow Manager**
- 방화벽 정책신청 관리

**FIRESCAN Collector**
- 방화벽 데이터 수집

**방화벽, 네트워크 장비**
- 정책/설정 연동
- Syslog 연동
- 통합로그솔루션 연동

# 2. 제품 사양




| 제품 | | Manager | | | Collector | Flow Manager | Analyzer |
|---|---|---|---|---|---|---|---|
| | | FSM 400 | FSM 2000 | FSM 5000 | FSC 2000 | | |
| 역할 | | • 방화벽 데이터 수집, 분석, 최적화, 통합관리 | | | • 방화벽 데이터 수집 | • 정책신청 관리 | • 방화벽 연동 |
| 사양 | CPU | • 4 Cores | • 8 Cores 이상 | • 16 Cores 이상 | • 8 Cores 이상 | • 8 Cores 이상 | • S/W License |
| | MEM | • 8 GB 이상 | • 32 GB 이상 | • 64 GB 이상 | • 32 GB 이상 | • 32 GB 이상 | |
| | HDD | • 1TB | • 1TB x 3 (RAID5) | • 1TB x 6 (RAID5) | • 1TB x 3 (RAID5) | • 1TB x 3 (RAID5) | |
| | Power | • Single | • Dual | • Dual | • Dual | • Dual | |



JMTRUE (주)제이엠트루

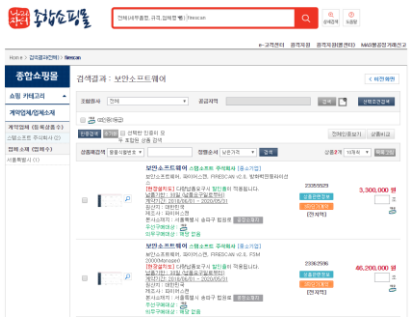
# 3. 인증

## • GS인증 1등급 제품


1등급 GOOD Software

| 항목 | 내용 |
|---|---|
| 소프트웨어의 명칭 | FIRESCAN v2.0 |
| 인 증 등 급 | 1 등급 |
| 인 증 번 호 | 18-0007 |
| 인 증 연 월 일 | 2018년 1월 4일 |
| 인 증 기 관 | 한국정보통신기술협회(TTA) |

## • 조달등록제품



✓ 우선구매대상

| 식별번호 | 규 격 명 | 납품기한 | 계약방법 |
|---|---|---|---|
| 23362596 | FSM 2000 (Manager) | 30일 (납품요구일로부터) | 3자단가계약 |
| 23355529 | 방화벽 연동 라이선스 | | |

# 4. Reference (구축)


## 정책 처리 속도 개선

- 중복정책(동일정책, 섀도우 정책 등) 및 장기간 사용하지 않는 정책을 제거

## 보안 위협 최소화

- 과다하게 허용된 정책, 내/외부 규정을 위반한 정책 제거

## 정책 입력 오류 최소화

- What-If 분석을 이용한 적용예정정책 자동 검증

## 업무 시간 단축

- 정책 신청프로세스 자동화

# 4. Reference (정책 최적화 컨설팅)

| 구분 | K 은행 | S 교육청 |
|---|---|---|
| 기 간 | 2017년 7월 ~ 8월 | 2017년 9월 ~ 10월 |
| 대 상 | 국산 2종 방화벽 00대 | 국산 2종 방화벽 00대 |
| 목 적 | 방화벽 관리현황을 분석하여 진단하여 개선안을 도출 | 방화벽 보안 정책 최적화를 통해 운영 서비스의 안정성 및 방화벽 운영의 효율적인 관리 향상 |
| 방 법 | 방화벽 정책과 로그를 실시간 수집하고 분석 | 방화벽 정책 분석 및 실시간/백업 로그 분석 |
| 내 용 | 중복정책, 사용률 분석, 위험 분석, 만료예정정책 분석 | 불필요 정책(미사용, 중복) 분석, 정책 사용 빈도 분석, 과다허용(보안 위협) 정책 분석 |
| 기 대 효 과 | • 중복정책과 일정 기간 사용하지 않는 정책에 대한 최적화 가이드를 제공하여 **정책 처리 속도 개선에 기여**<br>• 월 단위로 만료예정정책을 자동 분석 및 리포팅하여 **운영 효율 향상에 기여**<br>• 과다허용 정책에 대한 위험분석 및 실사용 추천 정책 제시로 **보안위협 최소화** | • 미사용 정책과 중복 정책(동일 정책, 섀도우 정책)에 대한 권고안을 제시하여 **정책 처리 속도 개선에 기여**<br>• 사용빈도가 많은 정책을 먼저 처리하는 정책 순서 재배치 방안을 제시하여 **방화벽 성능 향상에 기여**<br>• 과도하게 허용된 정책을 실제 사용하는 범위로 상세 분석하고 허용 범위를 최소화하는 권고안을 제시하여 **보안위협 제거에 기여** |

# 감사합니다.

㈜제이엠트루
Tel 02-2224-0925
Fax 02-2224-0935
hwkim@jmtrue.co.kr
www.jmtrue.co.kr
서울시 금천구 가산디지털1로 5, 2026-2호
(가산동, 대륭테크노타운 20차)